Web Share 3G 244WN

802.11n Wireless ADSL2+/3G Router

Manuale Utente

www.atlantis-land.com

Atlantis Land

INDICE

Atlantis Land

AVVERTENZE

Abbiamo fatto di tutto al fine di evitare che nel testo, nelle immagini e nelle tabelle presenti in questo manuale, nel software e nell'hardware fossero presenti degli errori. Tuttavia, non possiamo garantire che non siano presenti errori e/o omissioni. Infine, non possiamo essere ritenuti responsabili per qualsiasi perdita, danno o incomprensione compiuti direttamente o indirettamente, come risulta dall'utilizzo del manuale, software e/o hardware.

Il contenuto di questo manuale è fornito esclusivamente per uso informale, è soggetto a cambiamenti senza preavviso (a tal fine si invita a consultare il sito www.atlantisland.it o www.atlantis-land.com per reperirne gli aggiornamenti) e non deve essere interpretato come un impegno da parte di Atlantis Land che non si assume responsabilità per qualsiasi errore o inesattezza che possa apparire in questo manuale. Nessuna parte di questa pubblicazione può essere riprodotta o trasmessa in altra forma o con qualsiasi mezzo, elettronicamente o meccanicamente, comprese fotocopie, riproduzioni, o registrazioni in un sistema di salvataggio, oppure tradotti in altra lingua e in altra forma senza un espresso permesso scritto da parte di Atlantis Land. Tutti i nomi di produttori e dei prodotti e qualsiasi marchio, registrato o meno, menzionati in questo manuale sono usati al solo scopo identificativo e rimangono proprietà esclusiva dei loro rispettivi proprietari.

Restrizioni di responsabilità CE/EMC

Il prodotto descritto in questa guida è stato progettato, prodotto e approvato in conformità alle regole EMC ed è stato certificato per non avere limitazioni EMC.

Se il prodotto fosse utilizzato con un PC non certificato, il produttore non garantisce il rispetto dei limiti EMC. Il prodotto descritto è stato costruito, prodotto e certificato in modo che i valori misurati rientrino nelle limitazioni EMC. In pratica, ed in particolari circostanze, potrebbe essere possibile che detti limiti possano essere superati se utilizzato con apparecchiature non prodotte nel rispetto della certificazione EMC. Può anche essere possibile, in alcuni casi, che i picchi di valore siano al di fuori delle tolleranze. In questo caso l'utilizzatore è responsabile della "compliance" con i limiti EMC. Il Produttore non è da ritenersi responsabile nel caso il prodotto sia utilizzato al di fuori delle limitazioni EMC.

CE Mark Warning
In un ambiente domestico il dispositivo può causare interferenze radio, in questo caso è opportuno prendere le adeguate contromisure.

Dichiarazione di Conformità
Questo dispositivo è stato testato ed è risultato conforme alla direttiva 1999/5/CE del parlamento Europeo e della Commissione Europea, a proposito di apparecchiature radio e periferiche per telecomunicazioni e loro mutuo riconoscimento. Dopo l'installazione, la periferica è stata trovata conforme ai seguenti standard: EN 300.328(radio), EN 301 489-1, EN 301 489-17(compatibilità elettromagnetica) ed EN 60950(sicurezza). Questa apparecchiatura può pertanto essere utilizzata in tutti i paesi della Comunità Economica Europea ed in tutti i paesi dove viene applicata la Direttiva 1999/5/CE, senza restrizioni eccezion fatta per:

Francia(FR): Se si utilizza all'aperto tale dispositivo, la potenza in uscita è limitata (potenza e frequenza) in base alla tabella allegata. Per informazioni ulteriori consultare *www.art-telecom.fr*.

Luogo	Banda di Frequenze(MHz)	Potenza (EIRP)
Chiuso (senza restrizioni)	2400-2483,5	100mW(20dBm)
Aperto	2400-2454 2454-2483,5	100mW(20dBm) 10mW(10dBm)

Se l'uso di questa apparecchiatura in ambienti domestichi genera interferenze, è obbligo dell'utente porre rimedio a tale situazione.

Italia(IT): Questa periferica è conforme con l'Interfaccia Radio Nazionale e rispetta i requisiti sull'Assegnazione delle Frequenze. L'utilizzo di questa apparecchiatura al di fuori di ambienti in cui opera il proprietario, richiede un'autorizzazione generale. Per ulteriori informazioni si prega di consultare: *www.comunicazioni.it*.

Lussemburgo: Se utilizzato per servizi network o privati è da richiedere l'autorizzazione.

Norvegia (NO): apparecchiatura da non utilizzare in un aresa geografica di 20 km di raggio nei pressi di Ny Alesund.

Russia (CCP): solo per uso interno.

Dichiarazione di Conformità Sintetica CE ⓘ
Con la presente Sidin SpA dichiara che questo apparato è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttive 1999/5/CE. La dichiarazione di conformità nella sua forma completa è disponibile presso il sito www.atlantis-land.com (alla pagina del prodotto) o può essere richiesta a info@atlantis-land.com.

Importanti informazioni per il corretto riciclaggio/smaltimento di questa apparecchiatura

Le informazioni riportate sono redatte Ai sensi dell'art. 13 del Decreto Legislativo 25 luglio 2005, n. 151"Attuazione delle Direttive 2002/95/CE, 2002/96/CE e 2003/108/CE, relative alla riduzione dell'uso di sostanze pericolose nelle apparecchiature elettriche ed elettroniche, nonché allo smaltimento dei rifiuti".
Il simbolo qui sotto indicato, riportato sull'apparecchiatura elettronica e/o sulla confezione, indica che questa apparecchiatura elettronica non potrà essere smaltita come un rifiuto qualunque ma dovrà essere oggetto di raccolta separata.
Infatti i rifiuti di apparecchiatura elettroniche ed elettroniche devono essere sottoposti ad uno specifico trattamento, indispensabile per evitare la dispersione degli inquinanti contenuti all''interno delle apparecchiature stesse, a tutela dell'ambiente e della salute umana. Inoltre sarà possibile riutilizzare/riciclare parte dei materiali di cui i rifiuti di apparecchiature elettriche ed elettroniche sono composti, riducendo così l'utilizzo di risorse naturali nonché la quantità di rifiuti da smaltire.
La raccolta differenziata della presente apparecchiatura giunta a fine vita e' organizzata e gestita dal produttore. L'utente che vorrà disfarsi della presente apparecchiatura dovrà quindi contattare il produttore e seguire il sistema che questo ha adottato per consentire la raccolta separata dell'apparecchiatura giunta a fine vita. Si tenga presente che l'abbandono ed il deposito incontrollato di rifiuti sono puniti con sanzioni amministrative previste dalla norma vigente.

Il suo contributo nella raccolta differenziata dei rifiuti di apparecchiature elettriche ed elettroniche è essenziale per il raggiungimento di tutela della salute umana connessi al corretto smaltimento e recupero delle apparecchiature stesse.

AVVERTENZE
Utilizzare esclusivamente l'antenna fornita a corredo. Antenne diverse e/o con guadagno differente potrebbero violare le normative vigenti. Atlantis Land si intende sollevata da ogni responsabilità in caso di utilizzo di accessori (antenne e/o alimentatori) non contenuti nell'imballo.
Lasciare almeno 30cm di distanza tra l'antenna del dispositivo e l'utilizzatore.

1. Panoramica di prodotto

1.1 Visione d'insieme del WebShare 3G 244WN

Grazie per aver acquistato un prodotto Atlantis Land.
WebShare 3G 244 W300N è una soluzione all-in-one, che integra al suo interno un modem in standard ADSL2+ (fino a 24 Mbps in downstream e 2 Mbps in Upstream grazie al supporto Annex M), 4 porte Gigabit Ethernet, un Access Point ad altà velocità (fino a 300 Mbps) secondo le più recenti specifiche 802.11n ed una interfaccia di backup USB alla quale è possible collegare un modem 3G (HSDPA/GPRS/UMTS).
In questo documento verranno illustrate tutte le funzionalità messe a disposizione dal prodotto, Le quali rendono lo stesso adatto alle più svariate applicazioni professionali.

1.2 Contenuto della confezione

Prima di utilizzare il prodotto verificare che la confezione contenga:

- 1 x WebShare 3G 244WN
- 1 x Alimentatore esterno (15VDC @ 1.6A)
- 1 x Cavo UTP cat. 5 (connettore RJ-45)
- 1 x Cavo telefonico (connettore RJ-11)
- 1 x Cavo console PS2-RS 232
- 3 x Antenna rimovibile con connettore R-SMA
- 1 x Guida rapida multilingua (Italiano, Inglese e Francese)
- 1 x Cd-Rom contenente driver, utility e manuale multilingua
- 1 x Warranty Card
- 1 x WEEE Disclaimer

Qualora uno di questi componenti dovesse mancare è obbligatorio contattare immediatamente il rivenditore.

1.3 Caratteristiche tecniche

In questa sezione sono brevemente descritte le caratteristiche tecniche salient del prodotto:

- ***Accesso Internet ad alta velocità:*** WebShare 3G 244 WN integra al suo interno un modem ADSL2+, in grado di supportare un flusso in

downstream fino a 24 Mbps ed in upstream di 1 Mbps. Grazie a questa tecnologia sarà quindi possibile non solo navigare, ma anche usufruire di contenuti multimediali in alta definizione e di risorse gaming online nella maniera più semplice e veloce. Inoltre il pieno supporto dello standard Annex M consente di duplicare il flusso di trasferimento in upload.

- ***ADSL Multi-Mode Standard:*** Supporta in downstream un tasso di trasmissione fino 24Mbps ed un tasso di trasmissione in upstream sino a 1Mbps, inoltre soddisfa il Multi-Mode standard [ANSI T1.413, Issue 2; G.dmt (G.992.1); G.lite (G992.2); G.hs(G994.1); G.dmt.bis(ITU G.992.3); Gdmt.bisplus(ITU G.992.5)].
- ***Multi-Protocol per stabilire la connessione:*** Supporta PPPoA (RFC 2364 - PPP over ATM Adaptation Layer 5), RFC 1483 encapsulation over ATM (bridged oppure routed), PPP over Ethernet (RFC 2516), IPoA (RFC1577) per stabilire la connessione con l'ISP. Il prodotto supporta inoltre VC-based ed il LLC-based multiplexing.
- ***Gigabit Ethernet Switch:*** Lo switch Gigabit Ethernet integrato permette la realizzazione di reti locali ad alte performance, ritenute oggi una condizione necessaria per la condivisione di flussi ad alta definizione ed il trasferimento di contenuti di grosse dimensioni. Da oggi sarà difatti possibile sfruttare a pieno la massima velocità di tutte le periferiche presenti nella LAN, senza dove ricorrere all'utilizzo di un dispositivo aggiuntivo ed evitando cosi fastidiosi colli di bottiglia.
- ***Access Point 802.11n integrato:*** Grazie al dispositivo integrato, basato sulle più recenti specifiche 802.11n, il prodotto è in grado di fornire una connessione wireless fino a 6 volte più veloce e 3 volte più estesa di quelle attualmente disponibili tramite l'utilizzo di un Access Point 802.11b/g. Il pieno supporto hardware degli algoritmi di crittografia WPA/WPA2-PSK renderanno la vostra rete a prova di hacker, senza inficiare in alcun modo sulle prestazioni del prodotto in termini di risorse e di banda.
- ***Quick Installation Wizard:*** Grazie al supporto di un'interfaccia di configurazione via WEB l'apparato risulta essere facilmente configurabile. E' disponibile inoltre una comodissima Wizard che guida passo passo l'utente alla configurazione del Router.
- ***Universal Plug and Play (UPnP) e UPnP NAT Traversale:*** Grazie alla funzionalità UPnP è possibile configurare facilmente tutte quelle applicazioni che hanno problemi nell'attraversamento del NAT. L'utilizzo del

NAT Trasversale renderà le applicazioni in grado di autoconfigurarsi automaticamente senza l'intervento dell'utente.

- ***Network Address Translation (NAT):*** Consente a diversi utenti di accedere alle risorse esterne, come Internet, simultaneamente attraverso un indirizzo IP singolo. Sono inoltre supportate direttamente : ICQ, FTP, Telnet, E-mail, News, Net2phone, Ping, NetMeeting e altro.
- ***Extended Firewall con protezione da attacchi DoS e SPI:*** Il modulo firewall integrato all'interno del prodotto permette una protezione efficace dai più comuni attacchi hacker. Esso infatti è in grado di identificare e bloccare i più comuni attacchi DoS (Denial of Service), mentre un algoritmo avanzato di ispezione dei pacchetti (SPI) determina se lo stesso può avere accesso alla rete LAN o meno sulla base di criteri configurabili dall'utente.
- ***VLAN:*** Tale funzionalità permette di fatto di creare sottoreti indipendenti nella LAN aziendale. Questo innalza il livello di sicurezza e facilità l'intero processo di gestione della rete locale.
- ***QoS:*** Il Router ha la capacità di istradare con priorità prestabilite pacchetti in funzione della loro precedenza (IP e tipo di servizio). Sono proposte differenti classi di servizio.
- ***Sicurezza nei protocolli PPPoA e PPPoE:*** Il Router supporta infatti i protocolli PAP (Password Authentication Protocol) e CHAP (Challenge Handshake Authentication Protocol).
- ***Domain Name System (DNS) relay:*** Il Router intercettate le richieste DNS provvede a ruotarle all'opportune server DNS.
- ***Dynamic Domain Name System (DDNS):*** Il Client Dynamic DNS permette di associare ad un indirizzo IP dinamico (che vi viene di volta in volta assegnato dal server dell'ISP) un nome statico (host-name). E' necessario, per utilizzare il sevizio, effettuare una registrazione gratuita per esempio su http://www.dyndns.org/. Sono supportati differenti servizi DDNS.
- ***PPP over Ethernet (PPPoE):*** Il dispositivo offre il supporto per stabilire connessioni, con l'ISP, che usano il protocollo PPPoE. Gli utenti possono avere un accesso ad Internet ad alta velocità di cui condividono lo stesso indirizzo IP pubblico assegnato dall'ISP e pagano per un solo account. Non è richiesta l'installazione di nessun client software PPPoE per i PC locali.
- ***Virtual Server:*** L'utente può specificare alcuni servizi da rendere disponibili per utenti esterni. L'Adsl2+ VPN Router può riconoscere le

richieste entranti di questi servizi e rigirarle all'opportuno PC della Lan. E' possibile, per esempio, assegnare una data funzione ad un PC della Lan (come server Web) e renderlo disponibile in Internet (tramite l'unico IP statico disponibile). Dall'esterno è così possibile accedere al server Web che resta comunque protetto dal NAT. Grazie all'uso della tecnologia DDNS non è necessario che il Router abbia un abbonamento con IP fisso.

- ***Dynamic Host Control Protocol (DHCP) client and server:*** Lato WAN, il dispositivo può, grazie al DHCP client, prendere un indirizzo IP dall'ISP automaticamente. Nella LAN, il DHCP server può gestire sino a 253 client IP, distribuendo a ciascun PC un indirizzo IP, la subnet mask ed i DNS. Questa funzionalità consente una facile gestione della Lan.
- ***Protocollo RIP1/2 per il Routing:*** Supporto per una semplice tabella statica oppure il protocollo RIP1/2 per le capacità di routing.
- ***SNTP:*** Una facile via per avere informazioni sull'ora dal server SNTP.
- ***SNMP :*** E' possibile controllare il dispositivo utilizzando il protocollo SMTP V1/V2 o V3.
- ***Configurabile (GUI) via Web, Telnet o SNMP:*** La gestione e la configurazione sono possibili via interfaccia grafica (browser), via CLI (Telnet) o SNMP. L'apparato dispone di un comodo help in linea che aiuta l'utente. Supporta inoltre la funzione di management remota (Web, SNMP, Telnet) con la quale è possibile configurare e gestire il prodotto. Grazie all'uso della tecnologia DDNS non è necessario, per la gestione remota, che il Router abbia un abbonamento con IP fisso.

2. Uso del WebShare 3G 244WN

2.1 Precauzioni nell'uso di WebShare 3G 244WN

- Non usare il WebShare Router in un luogo in cui ci siano condizioni di alte temperatura ed umidità, il Router potrebbe funzionare in maniera impropria e danneggiarsi.
- Non usare la stessa presa di corrente per connettere altri apparecchi al di fuori del WebShare Router .
- Non aprire mai il case del WebShare Router né cercare di ripararlo da soli.

- Se il WebShare Router dovesse essere troppo caldo, spegnerlo immediatamente e rivolgersi a personale qualificato.
- Non appoggiare il dispositivo su superfici plastiche o in legno che potrebbero non favorire lo smaltimento termico.
- Mettere il WebShare Router su una superficie piana e stabile.
- Usare esclusivamente l'alimentatore fornito nella confezione, l'uso di altri alimentatori farà automaticamente decadere la garanzia.
- Non effettuare upgrade del firmare utilizzando apparati/client wireless ma solo wired. Questo potrebbe danneggiare il dispositivo ed invalidare la garanzia.

2.2 I LED frontali

LED	SIGNIFICATO
Power	• Acceso verde durante il corretto funzionamento. • Acceso rosso durante la fase di POST (Power On Self Test) o in caso di mancato caricamento del firmware (malfunzionamento dell'apparato)
Ethernet (1-4)	• Acceso verde in caso di collegamento a 1000 Mbps; • Acceso rosso in caso di collegamento a 100 Mbps; • Spento in caso di collegamento a 10 Mbps; • Lampeggiante in caso di

	trasmissione/ricezione dati.
USB	• Acceso verde in caso di corretto collegamento di un dispositivo USB (modem 3G). • Lampeggiante in caso di trasmissione/ricezione dati.
Wireless	• Accesso verde in caso di connessione attiva. • Lampeggiante in caso di trasmissione/ricezione dati. • Lampeggio regulare in fase di autenticazione WPS.
DSL	• Acceso verde fisso quando il modem è correttamente sincronizzato con il DSLAM. • Lampeggiante durante la fase di sincronizzazione.
Internet	• Accesso rosso in caso di errore in fase di autenticazione del profilo PPP. • Accesso verde indica la corretta autenticazione del profile PPP. • Lampeggiante in caso di trasmissione/ricezione dati. • Spento nel caso in cui il prodotto sia configurato in Bridge Mode oppure nel caso in cui non sia configurato alcun profilo PPP.

2.3 Le porte posteriori

PORTA	SIGNIFICATO

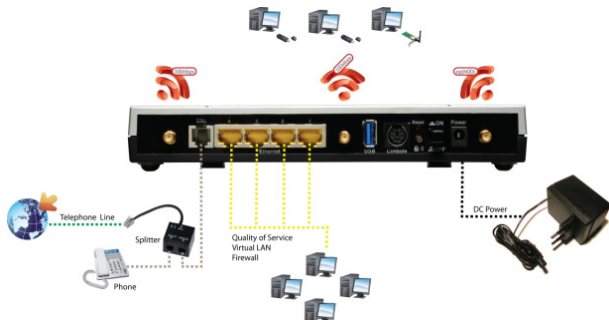
Antenna (3)	Collegare al connettore le antenne fornite a corredo.
DSL	Connettere il cavo RJ11 a questa porta per effettuare l'allacciamento all'ADSL.
Ethernet (1-4)	Connettere con un cavo UTP.
USB	Connettere il modem USB 3G.
Console	Connettere il cavo RS232 fornito alla porta seriale (9 pin) del PC. Tale connessione è opzionale.
WPS	Premere il pulsante per attivare il processo di sincronizzazione WPS (Wi-Fi Protected Setup).
Reset	Dopo che il dispositivo è acceso, premere per effettuare il reset o il restore. Le operazioni sono le seguenti: • **0-3 secondi:** per resettare il dispositivo • **3-6 secondi:** nessuna azione • **10 secondi o più:** effettua un ritorno alle condizioni di default (utilizzare, per esempio, in caso si perdesse la password).
Power	Pulsante di accensione/spegnimento.
Power Switch	Connettere l'alimentatore fornito a corredo a questo jack.

2.4 Modalità operative e cablaggio

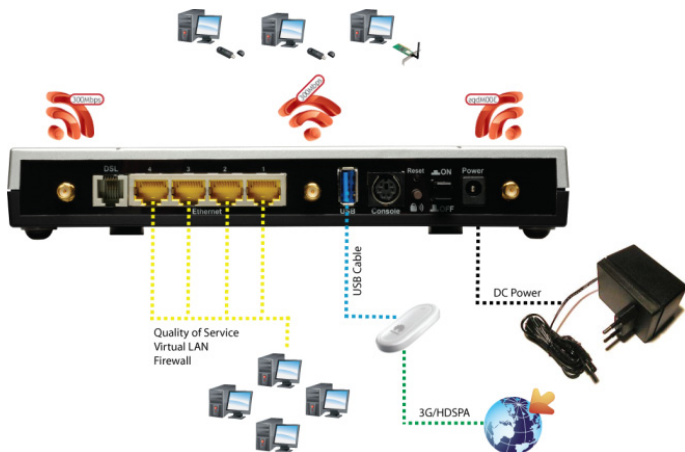
WebShare 3G 244 WN è dotato di una doppia interfaccia di connessione ADSL2+/3G (HSDPA/GPRS/UMTS); ognuna di esse può essere attivata come connessione primaria oppure, solo nel caso in cui la connessione principale sia quella ADSL2+ e sia disponibile una connessione 3G (tramite modem opzionale non incluso), è possible attivare la modalità ADSL WAN Backup, la quale permette il backup della connessione WAN over 3G nel caso di faiover temporaneo della linea ADSL, garantendo cosi una connessione sempre attiva (True Always-On Connection).

2.4.1 Connessione Single WAN ADSL

In questa modalità, WebShare 3G 244WN viene collegato e configurato come un tradizionale Router ADSL2+.
Nello specifico, per la realizzazione di un collegamento corretto, si prega di seguire la procedura indicata:

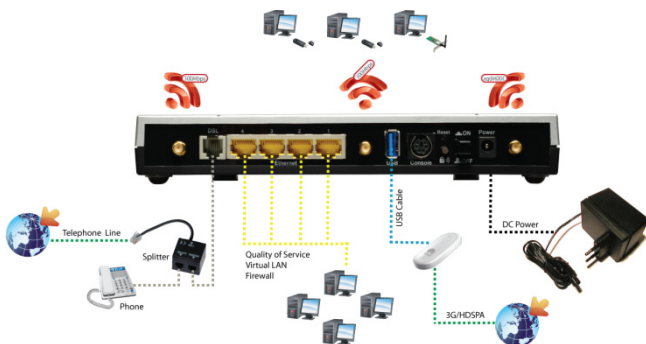
- Collegare il prodotto alla linea telefonica tramite il cavo telefonico RJ-11 fornito a corredo (potrebbe essere richiesta l'installazione di uno splitter ADSL al fine di minimizzare i disturbi sull'impianto telefonico).
- Collegare l'alimentatore fornito alla presa elettrica a muro ed al dispositivo tramite la porta POWER presente sul retro dello stesso.

2.4.2 Connessione Single WAN 3G

In questa modalità, WebShare 3G 244WN viene collegato ad un modem USB 3G e configurato come un Router 3G (HSDPA/GPRS/UMTS).
Nello specifico, per la realizzazione di un collegamento corretto, si prega di seguire la procedura indicata:

- Collegare un modem USB 3G alla porta USB 2.0 presente sulla parte posteriore del Router.
- Collegare l'alimentatore fornito alla presa elettrica a muro ed al dispositivo tramite la porta POWER presente sul retro dello stesso.

Il modem USB 3G non è incluso nell'offerta ed andrà acquistato separatamente. Si prega di verificare la compatibilità del modem acquistato tramite la lista presente al termine di questo manuale o reperibile sul sito www.atlantis-land.com presso la sezione dedicata al prodotto.

2.4.3 Connessione Dual WAN ADSL/3G con backup

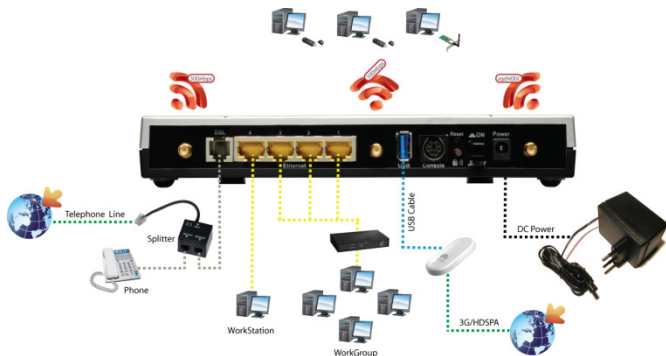
In questa modalità operativa, il WebShare 3G 244WN utilizzerà la connessione ADSL come principale ed in caso di disservizio temporaneo di quest'ultima, attiverà in maniera automatica il backup della connessione tramite interfaccia 3G.
Nello specifico, per la realizzazione di un collegamento corretto, si prega di seguire la procedura indicata:

- Collegare il prodotto alla linea telefonica tramite il cavo telefonico RJ-11 fornito a corredo (potrebbe essere richiesta l'installazione di uno splitter ADSL al fine di minimizzare i disturbi sull'impianto telefonico).
- Collegare un modem USB 3G alla porta USB 2.0 presente sulla parte posteriore del Router.
- Collegare l'alimentatore fornito alla presa elettrica a muro ed al dispositivo tramite la porta POWER presente sul retro dello stesso.

Il modem USB 3G non è incluso nell'offerta ed andrà acquistato separatamente. Si prega di verificare la compatibilità del modem acquistato tramite la lista presente al termine di questo manuale o reperibile sul sito www.atlantis-land.com presso la sezione dedicata al prodotto.

Si ricorda che questa modalità è disponibile solo nel caso in cui la connessione ADSL sia selezionata come connessione primaria; difatti, nel caso in cui il prodotto sia configurato per utilizzare l'interfaccia 3G come connessione primaria, tutte le funzionalità di backup non saranno disponibili.

2.4.4 Connessione alla rete LAN

Una volta terminata la parte di cablaggio relativa all'interfaccia WAN, è possibile focalizzare la propria attenzione sulle modalità di interfacciamento del WebShare 3G 244WN con una rete locale LAN preesistente oppure sulla creazione di una nuova rete locale LAN, ove il WebShare 3G 244WN fungerà da dispositivo responsabile della connettività dell'intera rete.
Riportiamo di seguito le modalità di connessione disponibili:

- Direttamente al PC tramite il cavo di rete LAN fornito a corredo.
- Tramite uno switch utilizzando il cavo di rete LAN fornito a corredo.
- Mediante una connessione wireless (IEEE 802.11b/g/n) utilizzando un client PCI/USB (come ad esempio quelli della serie NetFly 300).

Al termine delle operazioni di cablaggio fisico del prodotto, sarà possible avviare lo stesso mediante il pulsante POWER.
All'avvio, il dispositivo effettuerà un ciclo di diagnostica iniziale (delle durata di circa 60 secondi) al termine del quale sarà possibile utilizzare il WebShare 3G 244WN.
I Led frontali supporteranno l'utenza in una fase di diagnostica preliminare; lo stato degli stessi, al termine del processo di boot, dovrà essere come indicato di seguito:

LED	Stato
PWR	Acceso verde fisso
Ethernet 1-4	Acceso verde/arancio lampeggiante nel caso di dispositivi collegati
WLAN	Acceso verde lampeggiante
DSL	Acceso verde lampeggiante

A questo punto, sarà possibile accedere all'interfaccia di configurazione del prodotto.
Nel caso in cui il Router sia collegato alla medesima presa telefonica del telefono e/o nel caso in cui si rilevassero disturbi con gli apparecchi telefonici collegati alla stessa linea, si consiglia l'utilizzo di un filtro ADSL tripolare (A01-AF1) o RJ-45 (A01-AF2), in base alla tipologia delle prese telefoniche disponibili.

A01-AF2 (ADSL Splitter) ***A01-AF1 (Tripolar ADSL Filter)***

3. Informazioni preliminari

Il WebShare 3G 244WN può essere configurato via browser Web che dovrebbe essere incluso nel Sistema Operativo o comunque facilmente reperibile in Internet.
Prima di iniziare la configurazione del prodotto, è necessario ricevere dal proprio ISP il tipo di protocollo supportato per la connessione (PPPoE, PPPoA, RFC1483). Può essere utile, prima di iniziare, controllare di avere tutte le informazioni riportate nella tabella sottostante:

PPPoE	VPI/VCI, VC-based/LLC-based multiplexing, Username, Password, Service Name e indirizzo IP del Domain Name System (DNS) (può essere assegnato dall'ISP in maniera dinamica, oppure fisso).
PPPoA	VPI/VCI, VC-based/LLC-based multiplexing, Username, Password, and Domain Name e indirizzo IP del Domain Name System (DNS) (può essere assegnato dall'ISP in maniera dinamica, oppure fisso).
RFC1483 Bridged	VPI/VCI, VC-based/LLC-based multiplexing e configurare il dispositivo in BRIDGE.
RFC1483 Routed	VPI/VCI, VC-based/LLC-based multiplexing,indirizzo IP, Subnet mask, Gateway address, e indirizzi IP dei Domain Name System (DNS, sono IP fissi).

3.1 Impostazioni di fabbrica

Prima di iniziare la configurazione del WebShare 3G 244WN è necessario conoscere i parametri impostati in fase di produzione. Utilizzando questi settaggi e impostando i PC come client DHCP (come da istruzioni seguenti) ed infine configurando la connessione all'ISP (tutti i parametri della connessiona ADSL devono essere noti) è possibile utilizzare il WebShare 3G 244WN in pochissimo tempo. Per una configurazione dettagliata fare riferimento al manuale presente sul CD. Le configurazioni di Default del WebShare 3G 244WN sono:

- Username: **admin**
- Password: **atlantis**
- LAN IP Address: **192.168.1.254**
- Subnet Mask: **255.255.255.0**

- WAN: **PPPoA, VCMux, Routing, VPI=8, VCI=35**
- SSID: **A02-RAU244-W300N**, Sicurezza: **WPA-PSK**
- Chiave di autenticazione WPA: **WebShare244WN**
- **DHCP Server abilitato** (IP pool da 192.168.1.100 a 192.168.1.199)

Qualora si perdesse la password premere per 10 (o più) secondi il bottone reset (utilizzando un cacciavite a punta e premendo delicatamente) per far tornare il WebShare 3G 244WN alle impostazioni di default.

Di seguito un breve riepilogo delle configurazioni di fabbrica preimpostate e richiamabili in caso di reset del prodotto:

Wireless LAN	
SSID	A02-RAU244-W300N
Security	WPA-PSK
Security Passphrase	WebShare244WN
Wireless Mode	802.11n (20/40MHz)
Interfaccia LAN	
IP Address	192.168.1.254
Subnet Mask	255.255.255.0
DHCP Server	Abilitato
DHCP Server IP Pool	Da 192.168.1.100 a 192.168.1.100
Profilo WAN	
Encapsultation	PPPoA
Multiplexing	VC-Mux
Mode	Routing
VPI/VCI	8/35

3.2 Configurazione dello stack TCP/IP

Questa sezione descrive la configurazione richiesta dai singoli PC connessi alla LAN cui è connesso il WebShare 3G 244WN. Tutti i PC devono avere una scheda di rete Ethernet installata correttamente, essere connessi al Router ADSL direttamente o tramite un Hub/Switch ed avere il protocollo TCP/IP installato e correttamente configurato in modo da ottenere un indirizzo IP tramite il DHCP, oppure un indirizzo

IP che deve stare nella stessa subnet del Router ADSL. L'indirizzo IP di default è 192.168.1.254 e subnet mask 255.255.255.0.

3.2.1 Configurazione dei client in modalità DHCP

Certamente la strada più semplice per configurare i PC è quella settarli come client DHCP. In questa modalità l'IP (ed altri parametri) è assegnato dal Router ADSL.
Anzitutto è necessario preparare i PC inserendovi (qualora non vi fosse già) la scheda di rete. E' necessario poi installare il protocollo TCP/IP. Qualora il TCP/IP non fosse correttamente configurato, seguire gli steps successivi:

Qualsiasi workstation col TCP/IP può essere usata per comunicare con o tramite il WebShare 3G 244WN. Per configurare altri tipi di workstations fare riferimento al manuale del produttore.

Configurazione del client per Windows 2000

1. Andare su **Start -> Settings -> Control Panel**. Cliccare due volte su **Network and Dial-up Connections**.
2. Cliccare due volte su **Local Area Connection**.
3. In Local Area Connection Status cliccare **Properties**.
4. Selezionare Internet Protocol (TCP/IP) e cliccare su **Properties**.
5. Selezionare l'opzione **Obtain an IP address automatically** e successivamente **Obtain DNS server address automatically**.
6. Premere su **OK** per terminare la configurazione.

Configurazione del client per Windows XP

1. Andare su **Start** -> **Panello di Controllo**. Cliccare due volte su **Connessione di rete** (se non fosse presente cliccare prima su: Passa alla Visualizzazione Classica).
2. Cliccare due volte su **Connessione alla rete locale (LAN)**.
3. Nel TAB generale cliccare **Proprietà**.

4. Selezionare **Protocollo Internet (TCP/IP)** e cliccare su **Proprietà**.
5. Selezionare l'opzione **Ottieni automaticamente un indirizzo IP** e successivamente **Ottieni indirizzi server DNS automaticamente**.
6. Premere su **OK** per terminare la configurazione.

Configurazione del client per Windows Vista

1. Andare su **Start** -> **Pannello di Controllo** (cliccare sulla voce **Visualizzazione classica**) e qui cliccare due volte sull'icona **Centro Connessione di rete e Condivisione, poi** cliccare su **Gestisci connessione di rete.**
2. Cliccare 2 volte sull'icona **Local Area Connection** e cliccare su **Proprietà** poi cliccare su **Continua** (per continuare è necessaria l'utorizzazione dell'utente).
3. Selezionare **Protocollo Internet Versione 4 Protocol (TCP/IPv4)** e cliccare su **Proprietà.**
4. Selezionare l'opzione **Ottieni automaticamente un indirizzo IP** e successivamente **Ottieni indirizzi server DNS automaticamente**.
5. Premere su **OK** per terminare la configurazione.

Configurazione del client per MAC OS X

1. Cliccare sull'icona **Pannello di Controllo (mela)** nell'angolo in alto a sinistra dello schermo e selezionare la voce **Preferenze di Sistema**.
2. Cliccare ora sull'icona **Network**.
3. Selezionare la voce **Mostra: Ethernet Integrata** e cliccare sul pulsante **TCP/IP**.
4. Selezionare la voce **Utilizzo di DHCP** e chiudere il pannello.

Configurazione del client per Linux (KDE Interface)

1. Attivare il menu **System Settings**.
2. Selezionare l'opzione **Network Settings** all'interno del menù **Network and Connectivity**.

3. Selezionare l'interfaccia eth0 evidenziandola e cliccare sul pulsante **Configure Interface**.
4. Spuntare l'opzione **Automatic** e selezionare la modalità **DHCP** all'interno del menù TCP/IP.

Configurazione del client per Linux (GNOME Interface)

1. Cliccare sul menu **Sistema.**
2. Selezionare la voce **Amministrazione** e successivamente l'opzione **Rete**.
3. Evidenziare la voce **Connessione via cavo** e cliccare sul pulsante **Proprietà** per accedere alla configurazione della connessione.
4. All'interno della finestra di configurazione, impostare il parametro **Configurazione** sul valore **Configurazione automatica (DHCP)** e confermare premendo il pulsante **OK**.

3.2.2 Configurazione dei client in modalità IP statico

Questa tipologia di configurazione è dedicata agli amministratori di rete e/o ad un utenza esperta.

In reti mediamente complesse o a causa di necessità particolari (presenza di server sulla rete, necessità di pubblicazione di servizi WEB/FTP) può essere necessario configurare i client di rete con un indirizzamento IP statico, cosi da garantire alla macchina sempre lo stesso indirizzo IP anche in caso di riavvio del Router (e conseguente riavvio del server DHCP integrato).
Come per la configurazione in DHCP client, è innanzitutto necessario preparare i PC inserendovi (qualora non vi fosse già) la scheda di rete. E' necessario poi installare il protocollo TCP/IP e configurarlo seguenti gli steps successivi:

Configurazione del client per Windows 2000

1. Andare su **Start -> Settings -> Control Panel**. Cliccare due volte su **Network and Dial-up Connections**.
2. Cliccare due volte su **Local Area Connection**.

3. In Local Area Connection Status cliccare **Properties**.
4. Selezionare Internet Protocol (TCP/IP) e cliccare su **Properties**.
5. Selezionare l'opzione **Obtain an IP address automatically** e successivamente **Obtain DNS server address automatically**.
6. Premere su **OK** per terminare la configurazione.

Configurazione del client per Windows XP

1. Andare su **Start** -> **Panello di Controllo**. Cliccare due volte su **Connessione di rete** (se non fosse presente cliccare prima su: Passa alla Visualizzazione Classica).
2. Cliccare due volte su **Connessione alla rete locale (LAN)**.
3. Nel TAB generale cliccare **Proprietà**.
4. Selezionare **Protocollo Internet (TCP/IP)** e cliccare su **Proprietà**.
5. Selezionare l'opzione **Utilizza il seguente indirizzo IP** ed inserire un indirizzo IP congruente a quello impostato sull'interfaccia LAN del Router (es: 192.168.1.1, subnet 255.255.255.0, gateway 192.168.1.254).
6. Selezionare l'opzione **Utilizza i seguenti server DNS** ed impostare manualmente gli indirizzi DNS forniti dall'ISP.
7. Premere su **OK** per terminare la configurazione.

Configurazione del client per Windows Vista

1. Andare su **Start** -> **Pannello di Controllo** (cliccare sulla voce **Visualizzazione classica**) e qui cliccare due volte sull'icona **Centro Connessione di rete e Condivisione, poi** cliccare su **Gestisci connessione di rete.**
2. Cliccare 2 volte sull'icona **Local Area Connection** e cliccare su **Proprietà** poi cliccare su **Continua** (per continuare è necessaria l'utorizzazione dell'utente).
3. Selezionare **Protocollo Internet Versione 4 Protocol (TCP/IPv4)** e cliccare su **Proprietà.**

4. Selezionare l'opzione **Utilizza il seguente indirizzo IP** ed inserire un indirizzo IP congruente a quello impostato sull'interfaccia LAN del Router (es: 192.168.1.1, subnet 255.255.255.0, gateway 192.168.1.254)
5. Selezionare l'opzione **Utilizza i seguenti server DNS** ed impostare manualmente gli indirizzi DNS forniti dall'ISP.
6. Premere su **OK** per terminare la configurazione.

Configurazione del client per MAC OS X

1. Cliccare sull'icona **Pannello di Controllo (mela)** nell'angolo in alto a sinistra dello schermo e selezionare la voce **Preferenze di Sistema**.
2. Cliccare ora sull'icona **Network**.
3. Selezionare la voce **Mostra: Ethernet Integrata** e cliccare sul pulsante **TCP/IP**.
4. Selezionare la voce **Manualmente** ed inserire un indirizzo IP congruente a quello impostato sull'interfaccia LAN del Router (es: 192.168.1.1, subnet 255.255.255.0, gateway 192.168.1.254).

Configurazione del client per Linux (KDE Interface)

1. Attivare il menu **System Settings**.
2. Selezionare l'opzione **Network Settings** all'interno del menù **Network and Connectivity**.
3. Selezionare l'interfaccia eth0 evidenziandola e cliccare sul pulsante **Configure Interface**.
4. Spuntare l'opzione **Manual** ed inserire un indirizzo IP congruente a quello impostato sull'interfaccia LAN del Router (es: indirizzo IP 192.168.1.1, subnet mask 255.255.255.0).
5. Selezionare il menù a tendina **Routes** ed inserire l'indirizzo LAN del WebShare 3G 244WN (192.168.1.254) come Default Gateway.
6. Selezionare il menù a tendina **Domain Name** System, premere il pulsante **Add** ed inserire l'indirizzo del server DNS fornito dall'ISP.

Configurazione del client per Linux (GNOME Interface)

1. Cliccare sul menu **Sistema.**
2. Selezionare la voce **Amministrazione** e successivamente l'opzione **Rete**.
3. Evidenziare la voce **Connessione via cavo** e cliccare sul pulsante **Proprietà** per accedere alla configurazione della connessione.
4. All'interno della finestra di configurazione, impostare il parametro **Configurazione** sul valore **Indirizzo IP statico** ed inserire un indirizzo IP congruente a quello impostato sull'interfaccia LAN del Router (es: 192.168.1.1, subnet 255.255.255.0, gateway 192.168.1.254); confermare tramite il pulsante **OK**.
5. Selezionare il menu a tendina **DNS**, premere il pulsante **Aggiungi** nella parte relativa ai DNS Server ed inserire gli indirizzi forniti dall'ISP.

3.3 Verifica della configurazione TCP/IP

Per verificare il successo della configurazione (dopo aver riavviato il PC, operazione necessaria su Win98, 98Se,ME e invece sufficiente ottenere il rilascio dell'IP su XP, 2000), utilizzare il comando ping. Da una finestra Dos digitare:

ping 192.168.1.254

Se appare il seguente messaggio:

Pinging 192.168.1.254 with 32 bytes of data:
Reply from 192.168.1.254: bytes=32 times<10ms TTL=64
Reply from 192.168.1.254: bytes=32 times<10ms TTL=64
Reply from 192.168.1.254: bytes=32 times<10ms TTL=64

E' possibile procedere andando al punto seguente. Se invece appare il seguente messaggio:

Pinging 192.168.1.254 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.

Controllare che il led LAN sia acceso (cambiare il cavo qualora non fosse così). Controllare l'indirizzo del PC digitando winipcfg per (Win95,98,ME) o ipconfig (per Win2000,XP,VISTA) ed eventualmente reinstallare lo stack TCP/IP.

3.4 Configurazione del browser

Al fine di permettere la navigazione Internet tramite il WebShare 141W, di seguito riportiamo la configurazione necessaria per i più comuni browser presenti sul mercato:

Internet Explorer 7/8

1. Cliccare col tasto destro del mouse sull'icona e selezionare la voce **Proprietà**.
2. Selezionare la scheda Connessioni e spuntare l'opzione **Non utilizzare mai connessioni remote**.

Mozilla Firefox 3.0

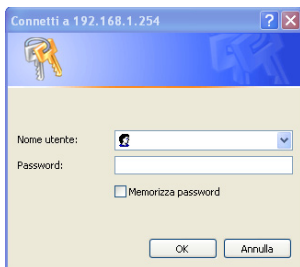
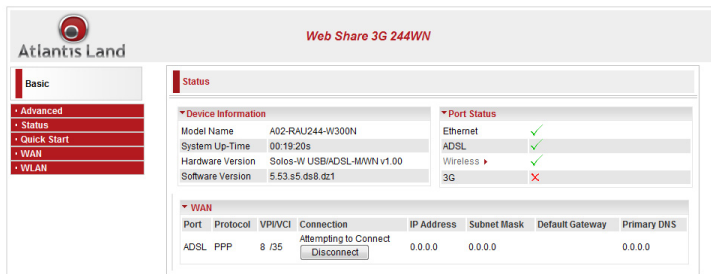
1. Avviare il browser Mozilla Firefox
2. Cliccare sulla **Strumenti** - >**Opzioni**
3. Selezionare la sezione **Avanzate**
4. Selezionare la scheda **Rete** -> **Connessioni**
5. Cliccare su **Impostazioni** e selezionare l'opzione **Nessun Proxy**.

Google Chrome

1. Avviare il browser Google Chrome.
2. Cliccare sull'icona e selezionare la voce **Opzioni**.
3. Selezionare la scheda Roba da Smanettoni e successivamente l'opzione **Rete** -> **Modifica impostazioni Proxy**.

3.5 Configurazione tramite Browser

Accedere tramite Internet Explorer al seguente indirizzo IP (dove si inserisce l'URL) che di default è: "**192.168.1.254**", e premere il tasto invio.

Utilizzare "**admin**" (come nome utente) e "**atlantis**" (come password). Premere OK per continuare.

4. Panoramica dell'interfaccia di configurazione

Al momento dell'accesso all'interfaccia di configurazione e gestione del dispositivo, verrà mostrata un interfaccia semplificata per la configurazione dei parametri basilari necessari alla navigazione (**Basic**) ed una sezione di configurazione avanzata (**Advanced**) per garantire il pieno controllo ed il più alto livello di configurabilità possibile.
Per comodità di consultazione, nel manuale verrà trattata la sola sezione **Advanced** mentre all'interno della guida rapida verrà trattata la sezione **Basic**; si ricorda che tutti i menu contenuti nella sezione Basic sono presenti anche nella sezione Advanced di cui per comodità di ricerca, di seguito viene riportata una tabella di associazione:

Basic Setup	Advanced Setup
Status	Status
Quick Start	Quick Start
WAN	Configuration - WAN – WAN Profile
WLAN	Configuration – LAN - Wireless

Al momento dell'accesso, verrà mostrato la seguente schermata:

Cliccare sul pulsante **Advanced** per attivare la modalità avanzata di gestione e configurazione del prodotto.

5. Status

In questa sezione sono riportati i parametri riguardanti le interfaccie LAN, WLAN, USB ed ADSL, ordinati in modo da permettere una semplice consultazione durante la fase di diagnostica di qualsiasi problematica oppure una visione d'insieme dello stato del Router.

Device Information

Parametro	Descrizione
Model Name	Visualizza il modello del prodotto.
Host Name	Visualizza il nome con il quale il prodotto verrà visto all'interno della rete LAN.
System Up-Time	Indica il tempo di attività del dispositivo dall'ultimo spegnimento e/o riavvio.
Current Time	Visualizza l'ora di sistema. Questo dato sarà il riferimento temporale con il quale verranno registrati i vari log.
Hardware Version	Visualizza l'identificativo della soluzione hardware utilizzata.
Software Version	Indica la versione di firmware correntemente in uso dal prodotto.

MAC Address	Indica il MAC Address associato all'interfaccia Ethernet del prodotto.

Port Status

Parametro	Descrizione
Ethernet	Indica lo stato di collegamento dell'interfaccia LAN.
ADSL	Indica lo stato di sincronizzazione della linea ADSL.
Wireless	Indica lo stato di funzionamento dell'interfaccia wireless.
3G	Indica lo stato di collegamento/funzionamento del modem 3G opzionale.

WAN

Parametro	Descrizione
Port	Indica l'interfaccia di connessione visualizzata.
Protocol	Indica il protocollo di connessione correntemente utilizzato.
VPI/VCI	Indica i valori di Virtual Path Identifier/Virtual Circuit Identifier associati al profilo di connessione.
Connection	Indica il tempo di attività della connessione dall'avvio del prodotto o dall'ultima disconnessione rilevata.
IP Address	Indica l'indirizzo IP attualmente associato all'interfaccia di connessione (ADSL/3G).
Subnet Mask	Indica la maschera di rete associata all'indirizzo visualizzato nel campo IP Address.
Default Gateway	Indica il valore del Default Gateway associato all'indirizzo visualizzato nel campo IP Address.
Primary DNS	Indica il valore del server DNS Primario.

Cliccando sui campi contenuti nella sezione **Port Status**, sarà possibile accedere ai parametri avanzati relativi ad ogni singola interfaccia.

Sono inoltre disponibili i pulsanti **Sync Now** per sincronizzare l'orologio interno del prodotto con un server SNTP esterno (fare riferimento al paragrafo **Configuration – System – Time Zone** per verificare l'attivazione del client) ed il pulsante **Connect/Disconnect** per gestire manualmente le operazioni di connessione/disconnessione del profilo PPP.

5.1 ADSL Status

Questa sezione, accessibile anche dalla sezione Port Status, mostra tutti i parametri relativi alla linea ADSL.

ADSL Status

Parameters	
DSP Firmware Version	E.25.41.55 A
Connected	true
Operational Mode	G.Dmt.BisPlus
Annex Type	AnnexA
Upstream	1291800
Downstream	23317300
Elapsed Time	0 day 0 hr 32 min 27 sec
SNR Margin(Upstream)	8.0 dB
SNR Margin(Downstream)	9.10 dB
Line Attenuation(Upstream)	0.0 dB
Line Attenuation(Downstream)	4.5 dB
CRC Errors(Upstream)	0
CRC Errors(Downstream)	0
Latency(Upstream)	Interleave
Latency(Downstream)	Interleave

Parametro	Descrizione
DSP Firmware Version	Indica la versione firmware del modulo DSP integrato.
Connected	Indica lo stato della connessione ADSL.
Operational Mode	Visualizza la modulazione correntemente in uso da parte del modem integrato.
Annex Type	Visualizza la tipologia Annex della linea ADSL.
Upstream	Indica il valore di picco della cella (PCR) in upstream.

Downstream	Indica il valore di picco della cella (PCR) in downstream.
SNR Margin	Visualizza il rapporto segnale/rumore (SNR) presente sulla linea.
Line Attenuation	Visualizza l'attenuazione di segnale presente sulla linea.
CRC Errors	Visualizza gli errori CRC ricevuti sull'interfaccia ADSL.
Latency	Indica la modalità di latenza della linea (Interleave o Fast).

5.2 3G Status

Questa sezione, accessibile anche dalla sezione Port Status, mostra tutti i parametri relativi all'interfaccia 3G opzionale.

Il modem USB 3G non è incluso nell'offerta ed andrà acquistato separatamente. Si prega di verificare la compatibilità del modem acquistato tramite la lista presente al termine di questo manuale o reperibile sul sito www.atlantis-land.com presso la sezione dedicata al prodotto.

▾3G Status

Parameters	
Status ▸	OK
Signal Strength	▮▮▮▮▮▮▮▮▮
Network Name	Telecom Italia M
Card Name	E169
Card Firmware	11.314.17.06.192
Current TX Bytes / Packets	0.5K / 21
Current RX Bytes / Packets	0.2K / 7
Total TX Bytes / Packets	1K / 45
Total RX Bytes / Packets	0.4K / 20

Clear

Parametro	Descrizione
Status	Indica lo stato di connessione del modem USB 3G:

	• **3G Card ready:** Modem USB correttamente rilevato; connessione non attiva. • **Connect:** Modem USB correttamente rilevato; connessione attiva. • **Closed:** Modem USB correttamente rilevato e disconnesso da Internet in seguito ad un failback della connessione ADSL. • **KO:** Modem USB non supportato.
Signal Strenght	Indica la potenza del segnale rilevato dal modem.
Network Name	Indica il nome identificativo della rete UMTS.
Card Name	Visualizza il modello del modem USB connesso.
Card Firmware	Visualizza la versione di firmware correntemente utiizzata dal modem 3G USB.
Current TX Bytes	Visualizza il traffico UMTS relativo alla connessione corrente.
Current RX Bytes	Visualizza il traffico UMTS relativo alla connessione corrente.
Total TX Bytes	Visualizza il traffico UMTS totale dall'accensione dell'apparato.
Total RX Bytes	Visualizza il traffico UMTS totale dall'accensione dell'apparato.

5.3 iBurst Status

Questa sezione visualizza una serie di parametri relativi alle chiavi wireless USB iBurst.

5.4 ARP Table

Questa sezione mostra la tabella ARP (Address Resolution Protocol) del dispositivo, riportando le associazioni MAC-IP, suddvise per tipologia. Atlantis Land consiglia la consultazione di questa sezione al fine di identificare correttamente gli eventuali indirizzi MAC da filtrare tramite la funzionalità MAC Address Filter (rif. capitolo Firewall).

▾ARP Table

Wired

IP Address	MAC Address	Interface	Static
192.168.3.150	00:17:42:75:38:fb	iplan	no
192.168.3.152	00:17:42:31:cf:4a	iplan	no
192.168.3.17	02:11:85:c4:22:d1	iplan	no

Wired

Parametro	Descrizione
IP Address	Visualizza una lista di indirizzi IP connessi al dispositivo.
MAC Address	Indica l'indirizzo MAC associato ad ogni indirizzo IP contenuto nel campo **IP Address**.
Interface	Visualizza l'interfaccia alla quale risultano collegate le periferiche indicate.
Static	Indica se l'associazione MAC-Indirizzo IP è dinamica (quindi creata autonomamente dal Router all'avvio) oppure statica (impostata dall'utente in maniera permanente).

Wireless

Parametro	Descrizione
IP Address	Visualizza una lista di indirizzi IP connessi al dispositivo.
MAC Address	Indica l'indirizzo MAC associato ad ogni indirizzo IP contenuto nel campo **IP Address**.

5.5 DHCP Table

Tramite questa sezione è possibile visualizzare le associazioni DHCP rilasciate dal Router suddivise in categorie (attive, scadute e permanenti).

Type

Parametro	Descrizione
Leased	Visualizza gli indirizzi IP assegnati.
Expired	Visualizza le associazioni DHCP scadute.
Permanent	Visualizza le associazione DHCP permanenti impostate dall'utente.

Leased Table, Expired Table, Permanent Table

Parametro	Descrizione
IP Address	Indica l'indirizzo IP rilasciato dal DHCP Server

MAC Address	Indica l'indirizzo MAC al quale è associato l'indirizzo presente nel campo **IP Address**.
Client Host Name	Indica il nome identificativo della macchina associata all'indirizzo MAC indicato nel campo **MAC Address**.
Expiry	Indica il tempo rimanente prima della scadenza dell'indirizzo IP indicato nel campo **IP Address**.

5.6 Routing Table

Routing Table

Routing Table

Valid	Destination	Netmask	Gateway/Interface	Cost
✓	0.0.0.0	0.0.0.0	0.0.0.0/ ipwan	1

RIP Routing Table

Destination	Netmask	Gateway	Cost
0.0.0.0	0.0.0.0	0.0.0.0	1

Routing Table

Parametro	Descrizione
Valid	Indica la validità della rotta statica.
Destination	Indica la rete di destinazione impostata nella rotta statica selezionata.
Netmask	Indica la maschera di rete della rete di destinazione.
Gateway/Interface	Indica l'indirizzo del gateway o dell'interfaccia da utilizzare per raggiungere la rete di destinazione.
Cost	Indica il numero di hop necessario per raggiungere la rete di destinazione.

RIP Routing Table

Parametro	Descrizione
Destination	Indica la rete di destinazione impostata nella rotta statica selezionata.
Netmask	Indica la maschera di rete della rete di destinazione.
Gateway/Interface	Indica l'indirizzo del gateway o dell'interfaccia da utilizzare per

	raggiungere la rete di destinazione.
Cost	Indica il numero di hop necessario per raggiungere la rete di destinazione.

5.7 NAT Sessions

Questa sezione riepiloga tutte le sessioni di NAT aperte tra l’interfacccia esterna (WAN) e quella interna (LAN) al momento della visualizzazione.

▾NAT Sessions

```
   TCP :    0 sessions, Default Timeout   1800 Seconds
   UDP :    3 sessions, Default Timeout    120 Seconds
Others :    0 sessions, Default Timeout     60 Seconds
 Total :    3 sessions
```

Refresh   Page: 1

Il dispositivo in questione permette la gestione di 1500 sezioni NAT simultanee. Il Router non riesce a costruire, per mancanza di risorse, altre sessioni se questo limite è raggiunto.

5.8 UPnP Portmap

Questa sezione visualizza tutti le mappature attualmente attive da parte di dispositive/programmi, che utilizzano la tecnologia UPnP. Si prega di fare riferimento alla sezione **Advanced** per la configurazione dei parametri UPnP per il prodotto.

UPnP Portmap

UPnP Portmap Table					
Name	Protocol	External Port	Redirect Port	IP Address	Duration(s)
item0	17	7498	7498	192.168.3.182	Always On
item1	6	7498	7498	192.168.3.182	Always On

Parametro	Descrizione
Name	Indica il nome identificativo della regola.
Protocol	Indica il numero del protocollo utilizzato (es: TCP=6)
External Port	Indica il numero di porta servizio su cui è atteso il pacchetto
Redirect Port	Indica il numero di porta servizio sul quale verrà reindirizzato il pacchetto
IP Address	Indica l'indirizzo IP lato LAN verso il quale verrà instradato il pacchetto
Duration(s)	Indica la durata della regola indicata.

5.9 Event Log

Questa pagina visualizza il registro di log del prodotto. Gli eventi di rilievo (come ad esempio le disconnessioni della linea ADSL, rilevamento di un'eventuale minaccia per il sistema , etc) vengono tracciati in questa finestra. Si prega di fare riferimento alla sezione **Configuration – Firewall** per l'attivazione dei relativi strumenti di logging.

Event Log

```
----------- system log buffer head --------------
Jan 01 00:00:10 home.gateway:im:none: Changed iplan IP address to 192.168.1.254
Jan 03 01:00:01 home.gateway:im:none: Reset SNMP community to factory default
settings
Jan 03 01:00:30 home.gateway:turbo_extEvtHandlerProc:none: ADSL line is UP!
Jan 03 01:00:40 home.gateway:webserver:none: Changed iplan IP address to
192.168.3.29
Jan 03 01:22:14 home.gateway:turbo_extEvtHandlerProc:none: ADSL line is DOWN!
Jan 03 01:27:04 home.gateway:turbo_extEvtHandlerProc:none: ADSL line is UP!
Jan 03 01:28:06 home.gateway:scanpvc:none: Starting PVC scan
Jan 03 01:29:11 home.gateway:scanpvc:none: Starting PVC scan
Jan 03 01:36:32 home.gateway:ppp:none: Channel Id(0) connected
Jan 03 01:36:32 home.gateway:im_backend:none: Changed ipwan IP address to
192.168.5.199

----------- system log buffer tail --------------
```

Refresh Clear

E' possibile interrogare e memorizzare i dati tramite un SysLog esterno. Per ulteriori dettagli, fare riferimento all'appendice relativa.

5.10 Error Log

Questa pagina visualizza il registro degli errori rilevati dal Router (ad esempio, nome non valido assegnato ad una regola, etc).

Error Log		
Error Log (*times are in seconds since last reboot*)		
When	Process	Error Log

5.11 Diagnostic

Questa schermata riporta un breve test diagnostico per la verifica del corretto funzionamento e configurazione del dispositivo.

Diagnostic	
LAN Connection	
Testing Ethernet LAN connection	PASS
Testing Wireless LAN connection	PASS
WAN Connection	
Testing ADSL Synchronization	PASS
Testing WAN connection	PASS
Ping Primary Domain Name Server	PASS
PING www.google.com	FAIL
Refresh	

Nel caso in cui tutti i test risultino positivi ed il solo step Ping www.google.com risulti fallito, si prega di controllare l'impostazione dei server DNS sulla propria macchina.

6. Quick Start

Si ricorda che tramite la procedura Quick Start non sarà possibile configurare la connessione in modalità ADSL WAN Backup.

Per avviare la procedura, cliccare sul tasto **Quick Start** e seguire le indicazioni riportate di seguito.

6.1 Configurazione Single WAN ADSL

Dopo aver verificato la correttezza del cablaggio (fare riferimento al paragrafo **Modalità operative e cablaggio**), è necessario configurare il Router come segue:

1. Impostare il campo **Connect Mode** in **ADSL** per impostare l'interfaccia ADSL come connessione primaria verso la rete Internet.

2. Selezionare l'opzione **Auto** e premere **Apply**. Il sistema avvierà una procedura di auto rilevamento della connessione ADSL ed al termine mostrerà la schermata di configurazione ADSL. Selezionando l'opzione **Manually**, sarà possibile configurare manualmente i parametri di linea.
   Nel caso in cui siano disponibili profili multipli, il sistema mosterà una finestra riepilogativa di questi ultimi. Selezionare il profilo corretto in accordo con i dati di linea forniti dall'Internet Service Provided (ISP).

3. A questo punto sarà necessario configurare l'interfaccia ADSL per la connessione secondo i parametri forniti dal proprio ISP.

6.1.1 PPPoE

▾ WAN Port (WAN > Wireless)

Connection	
Profile Port	ADSL ▾
Protocol	PPPoE (RFC2516, PPP over Ethernet) ▾
VPI/VCI	8 / 35
Username	
Password	
Service Name	
Auth. Protocol	Chap(Auto) ▾
MTU	1492
IP Address	0.0.0.0 ('0.0.0.0' means 'Obtain an IP address automatically')
Obtain DNS automatically	☑ Enable
Primary DNS/Secondary DNS	0.0.0.0 / 0.0.0.0
Apply	

Configurare il WebShare 3G 244WN come da figura, inserendo nei campi relativi le credenziali di accesso (Username, Password) fornite dall'ISP.

L'apparato validerà a questo punto la connessione appena creata. In caso di problemi, controllare i parametri della connessione e verificarne la correttezza con il Provider.

Si ricorda che tale dispositivo non è adatto a gestire abbonamenti non FLAT o a consumo. Atlantis Land non potrà essere ritenuta responsabile per qualsiasi problematica derivante dall'utilizzo di abbonamenti a consumo (non FLAT) o da una errata configurazione dell'apparato. **In caso di dubbio contattare preventivamente l'assistenza tecnica.**

In caso di Protocollo PPPoE, potrebbe essere necessario cambiare il valore del campo **MTU** con un valore 1492 o minore.

6.1.2 PPPoA

WAN Port (WAN > Wireless)

Connection	
Profile Port	ADSL
Protocol	PPPoE (RFC2516, PPP over Ethernet)
VPI/VCI	8 / 35
Username	
Password	
Service Name	
Auth. Protocol	Chap(Auto)
MTU	1492
IP Address	0.0.0.0 ('0.0.0.0' means 'Obtain an IP address automatically')
Obtain DNS automatically	☑ Enable
Primary DNS/Secondary DNS	0.0.0.0 / 0.0.0.0

Apply

Configurare il WebShare 3G 244WN come da figura, inserendo nei campi relativi le credenziali di accesso (Username, Password) fornite dall'ISP.

L'apparato validerà a questo punto la connessione appena creata. In caso di problemi, controllare i parametri della connessione e verificarne la correttezza con il Provider.

Si ricorda che tale dispositivo non è adatto a gestire abbonamenti non FLAT o a consumo. Atlantis Land non potrà essere ritenuta responsabile per qualsiasi problematica derivante dall'utilizzo di abbonamenti a consumo (non FLAT) o da una errata configurazione dell'apparato. **In caso di dubbio contattare preventivamente l'assistenza tecnica.**

6.1.3 MPOA (RFC 1483)

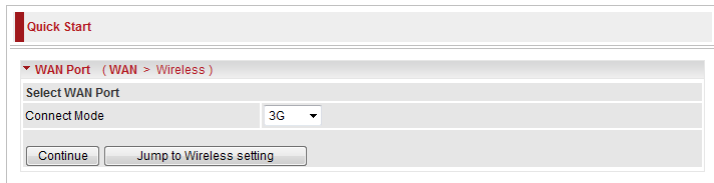
Questa configurazione è valida nel caso di abbonamento con 1 IP statico e NAT attivo (per la gestione della classe pubblica fare riferimento al manuale su CD).

▾ WAN Port (WAN > Wireless)

Connection	
Profile Port	ADSL
Protocol	MPoA (RFC1483/RFC2684, Multiprotocol Encapsulation over AAL5)
VPI/VCI	8 / 35
Encap. Method	LLC Routed
MTU	1500
IP Address	0.0.0.0 ('0.0.0.0' means 'Obtain an IP address automatically')
Subnet Mask	0.0.0.0
Default Gateway	
Obtain DNS automatically	☑ Enable
Primary DNS/Secondary DNS	0.0.0.0 / 0.0.0.0
Apply	

Configurare il WebShare 3G 244WN come da figura, inserendo nei campi relativi le credenziali (indirizzo IP, Subnet Mask e Gateway) fornite dall'ISP.

6.1.4 IPoA/PURE BRIDGE/MULTIPLE SESSION

Queste modalità di connessione avanzate non vengono descritte in quanto di uso molto rado. In caso di necessità, consultare il paragrafo Supporto al termine di questo manuale.

La modalità **Pure Bridge**, permette al WebShare 3G 244WN di essere utilizzato come un modem Ethernet. Sarà quindi necessaria la presenza di uno stack PPPoE installato sul PC per poter stabilire una connessione a banda larga.

6.2 Configurazione Single WAN 3G

Dopo aver verificato la correttezza del cablaggio (fare riferimento al paragrafo **Modalità operative e cablaggio**), è necessario configurare il Router come segue:

1. Impostare il campo **Connect Mode** in **3G** per impostare l'interfaccia 3G come connessione primaria verso la rete Internet.

2. A questo punto sarà necessario configurare l'interfaccia 3G per la connessione secondo i parametri forniti dal proprio operatore di telefonia mobile.

Di seguito sono riportate le configurazioni utilizzabili con tutti i maggiori provider di telefonia mobile nazionali; per alcune tipologie di contratto non recenti o per alcune opzioni Business, i parametri potrebbero subire variazioni rispetto ai dati riportati.
Si consiglia la verifica dei dati di connessione necessari prima di intraprendere la configurazione del WebShare 3G 244WN

Il modem USB 3G non è incluso nell'offerta ed andrà acquistato separatamente. Si prega di verificare la compatibilità del modem acquistato tramite la lista presente al termine di questo manuale o reperibile sul sito www.atlantis-land.com presso la sezione dedicata al prodotto.

Si ricorda che tale dispositivo non è adatto a gestire abbonamenti non FLAT o a consumo. Atlantis Land non potrà essere ritenuta responsabile per qualsiasi problematica derivante dall'utilizzo di abbonamenti a consumo (non FLAT) o da una errata configurazione

dell'apparato. **In caso di dubbio contattare preventivamente l'assistenza tecnica.**

6.2.1 VODAFONE

WAN Port (WAN > Wireless)

Connection	
Profile Port	3G
iBurst	☐ Enable
Mode	UMTS first
APN	web.omnitel.it
Username	
Password	
Auth. Protocol	Chap(Auto)
MTU	1500
PIN	
Obtain DNS automatically	☑ Enable
Primary DNS/Secondary DNS	0.0.0.0 / 0.0.0.0

Warning: Entering the wrong PIN code three times will lock the SIM.

Apply

Per la configurazione dell'interfaccia per l'utilizzo con modem 3G Vodafone, configurare il WebShare 3G 244WN come riportato in figura.

Nel caso in cui la SIM card sia protetta dal codice di sicurezza PIN, immettere questo valore nel campo **PIN**.

Attenzione: L'immisione di un codice PIN errato per 3 volte porterà al blocco della SIM card.

6.2.2 TIM (Telecom Italia Mobile)

▼ WAN Port (WAN > Wireless)

Connection	
Profile Port	3G
iBurst	☐ Enable
Mode	UMTS first
APN	ibox.tim.it
Username	
Password	
Auth. Protocol	Chap(Auto)
MTU	1500
PIN	
Obtain DNS automatically	☑ Enable
Primary DNS/Secondary DNS	0.0.0.0 / 0.0.0.0

Warning: Entering the wrong PIN code three times will lock the SIM.

Apply

Per la configurazione dell'interfaccia per l'utilizzo con modem 3G TIM, configurare il WebShare 3G 244WN come riportato in figura.

Nel caso in cui la SIM card sia protetta dal codice di sicurezza PIN, immettere questo valore nel campo **PIN**.

Per alcune particolari tipologie di contratto poco recenti, la registrazione al servizio 3G può essere attivata manualmente richiedendo il servizio direttamente al proprio operatore di telefonia mobile.

In questi casi è possibile che il valore del campo APN vada variato in **uni.tim.it**

Attenzione: L'immisione di un codice PIN errato per 3 volte porterà al blocco della SIM card.

6.2.3 WIND

▾ WAN Port (WAN > Wireless)

Connection	
Profile Port	3G
iBurst	☐ Enable
Mode	UMTS first
APN	internet.wind
Username	
Password	
Auth. Protocol	Chap(Auto)
MTU	1500
PIN	
Obtain DNS automatically	☑ Enable
Primary DNS/Secondary DNS	0.0.0.0 / 0.0.0.0
Warning: Entering the wrong PIN code three times will lock the SIM.	
Apply	

Per la configurazione dell'interfaccia per l'utilizzo con modem 3G WIND, configurare il WebShare 3G 244WN come riportato in figura.

Nel caso in cui la SIM card sia protetta dal codice di sicurezza PIN, immettere questo valore nel campo **PIN**.

Per alcune particolari tipologie di contratto business, i dati di connessione potrebbero subire variazioni rispetto alla configurazione riportata in figura.

In caso di malfunzionamento della connessione, si consiglia di provare a sostituire il valore del campo APN con **internet.wind.biz**

Attenzione: L'immisione di un codice PIN errato per 3 volte porterà al blocco della SIM card.

6.2.4 TRE (H3G)

▾ WAN Port (WAN > Wireless)

Connection	
Profile Port	3G
iBurst	☐ Enable
Mode	UMTS first
APN	tre.it
Username	
Password	
Auth. Protocol	Chap(Auto)
MTU	1500
PIN	
Obtain DNS automatically	☑ Enable
Primary DNS/Secondary DNS	0.0.0.0 / 0.0.0.0

Warning: Entering the wrong PIN code three times will lock the SIM.

Apply

Per la configurazione dell'interfaccia per l'utilizzo con modem 3G TRE, configurare il WebShare 3G 244WN come riportato in figura.

Nel caso in cui la SIM card sia protetta dal codice di sicurezza PIN, immettere questo valore nel campo **PIN**.

L'operatore in oggetto potrebbe necessitare di parametri di connessione differenti in base alla tipologia di SIM utilizzata (Dati oppure Ricaricabile). Nel caso di utilizzo di SIM di tipo Dati, impostare il campo APN con il valore **datacard.tre.it**.

Attenzione: L'immisione di un codice PIN errato per 3 volte porterà al blocco della SIM card.

6.3 Configurazione Wireless

Configurare ora i parametri relative alla rete wireless, impostando nel campo SSID il nome da assegnare alla rete (è possibile mantenere quello di default), il canale da utilizzare per la trasmissione ed eventualmente sostituire la chiave di protezione associata al profilo WPA-PSK.

Atlantis Land consiglia la sostituzione della chiave WPA-PSK all'atto della prima configurazione in modo da garantire un alto livello di protezione della rete wireless e LAN.

Nel caso in cui nell'ambiente circostante siano operativi altri Access Point / Router Wireless, potrebbe essere necessario cambiare il canale di trasmissione al fine di migliorare le performance del WebShare 3G 244WN.

L'errata configurazione del campo Regulation Domain può indurre il WebShare 3G 244WN alla trasmissione al di fuori dei limiti di potenza e frequenza imposti dalle leggi nazionali.
Atlantis Land non si riterrà responsabile in alcun modo in caso di errata configurazione dell'apparato.

6.4 Salvataggio delle impostazioni

Al termine della configurazione guidata, il prodotto provvederà al salvataggio dei parametri nella memoria FLASH in modo tale da rendere definitive le configurazioni.

Quick Start

WAN Port (WAN > Wireless)

Process finished

Success.

The Quick Start process is finished. Your device has been successfully configured.

7. Configuration

Questa sezione permette di accedere alla configurazione di tutte le funzionalità contenute all'interno del prodotto.

7.1 LAN – Local Area Network

In questa sezione è possibile configurare le interfaccie Ethernet e Wireless del prodotto.

7.1.1 Bridge Interface

Atlantis Land consiglia l'utilizzo di questa funzionalità solo ad utenze esperte. Un'errata configurazione delle VLAN potrebbe rendere non raggiungibile il prodotto e rendere necessario un ripristino delle configurazioni di fabbrica del dispositivo.

In questa sezione è possibile impostare le porte fisiche facenti parte di ogni singola interfaccia bridge. Questa funzionalità, associata alla funzione VLAN (maggiori dettagli sono reperibili nel paragrafo dedicato) permettono di eseguire alcune configurazioni di carattere avanzato, quali configurazione contemporanea di più profili PVC per la gestione di abbonamenti triple-play od isolamento di segmenti di rete.

Parameters

Parametro	Descrizione
P(1-4)	Identifica la porte Ethernet fisiche integrate nel dispositivo.
Wireless	Identifica l'interfaccia wireless.

Device Management

Parametro	Descrizione
Management Interface	Identifica l'interfaccia abilitata alle operazione di management del dispositivo.

Solo l'interfaccia eletta come interfaccia di Management sarà sottoposta alle policy di NAT/NAPT (con conseguente possibilità di navigazione) e sarà abilitata alla configurazione WEB dell'apparato.

Di seguito sono riportate le configurazioni possibili:

Interfaccie Bridge	VLAN Port
ethernet	P1 / P2 / P3 / P4 / Wireless
ethernet1	P2 / P3 / P4 / Wireless
ethernet2	P3 / P4 / Wireless
ethernet3	P4 / Wireless
ethernet4	Wireless

Se un PC appartiene alla VLAN1 non potrà vederne un altro connesso su una porta appartenente alla VLAN2.

Cliccando su una delle interfaccie, è possibile accedere alla configurazione avanzata impostando la tipologia dei pacchetti accettati (se con TAG o senza) , la tipologia di filtro, e su quale VLAN indirizzare i pacchetti sprovvisti di TAG.

Fare riferimento all'appendice relativa per la configurazione approfondita delle Virtual LAN (VLAN).

7.1.2 Ethernet

Parametro	Descrizione
IP Address	Inserire l'indirizzo IP da assegnare all'interfaccia LAN del prodotto.
Subnet Mask	Inserire la subnet mask da associare al campo sopra indicato.
RIP	Selezionare questa opzione se si desidera abilitare il protocollo RIP e selezionare il tipo di protocollo RIP che si desidera utilizzare (**RIP v1**, **RIP v2** o **RIP v2 Multicast**).

7.1.3 IP Alias

Questa sezione permette la creazione di molteplici interfaccie IP virtuali associabili a differenti interfaccie logiche al fine di poter interconnettere due o più LAN con classi differenti ad una stessa connessione Internet senza ricorrere ad un dispositivo broadband.

Parametro	Descrizione

IP Address	Inserire l'indirizzo IP da assegnare all'interfaccia virtuale.
Subnet Mask	Inserire la subnet mask da associare al campo sopra indicato.
Security Interface	Specificare la policy di firewall alla quale sottoporre l'interfaccia virtuale: • **Internal:** Questa interfaccia risulterà sottoposta a NAT. Tutto in traffico generato da questa interfaccia verrà sottoposto ad un processo di Address Translation prima di essere instradato in Internet. • **External:** Questa interfaccia non risulterà sottoposta a NAT, pertanto tutto il traffico generato verrà propagato in Internet senza essere sottoposto ad alcun processo. Questa tipologia di interfaccia viene utilizzata nel caso di abbonamenti di tipo business nei quali viene fornita una classe di indirizzamenti IP pubblici. • **DMZ:** Imposta questa rete come DMZ. L'interfaccia non è sottoposta ad alcun NAT ed è direttamente esposta verso Internet.

Si prega di fare riferimento all'appendice relativa per una configurazione dettagliata della funzionalità Multi-NAT.

Per modificare un'interfaccia, selezionarla tramite la colonna **Edit** ed eseguire le modifiche necessarie; al termine premere il tasto **Edit/Delete** per applicare le modifiche.

Per eliminare un'interfaccia, selezionarla tramite la colonna **Delete** e premere il tasto **Edit/Delete** per confermare l'eliminazione.

7.1.4 Ethernet Client Filter

Questa sezione permette di configurare una policy di filtraggio basata sugli indirizzamento MAC dei dispositive collegati via cavo al Router al fine di inibire accessi non autorizzati alla rete LAN.
Le politiche di filtering attivabili si riassumono come segue:

- **Blocca tutto tranne ciò che viene esplicitamente dichiarato:** utilizzando questo metodo, il dispositivo bloccherà l'accesso a qualsiasi dispositivo non sia specificatamente dichiarato nella MAC Address List.
- **Permettere tutto tranne ciò che viene esplicitamente dichiarato:** in questo caso, il prodotto permetterà l'accesso a qualsiasi dispositivo non sia specificatamente dichiarato nella MAC Address List.

Il prodotto supporta fino a 16 regole di filtraggio (non è configurato alcun preset di fabbrica) configurabili come segue:

Parametro	Descrizione
Ethernet Client Filter	Selezionare la policy tra le seguenti: • **Disable:** la funzionalità non è abilitata • **Allowed:** In questo caso, il dispositivo negherà

	l'accesso alla rete a tutti i dispositivi non specificatamente riportati nel campo MAC Address List. • **Blocked:** In questo caso, il dispositivo permettà l'accesso alla rete a tutti i dispositivi non specificatamente riportati nel campo MAC Address List, bloccando quelli presenti nel campo MAC Address List.
Mac Address List	Impostare gli indirizzi MAC che si desidera bloccare o permettere, in relazione alla tipologia di filtraggio precedentemente selezionata.

Al fine di facilitare l'inserimento degli indirizzamenti MAC da filtrare, premendo il tasto Candidates ▸ sarà possibile visualizzare una lista delle periferiche attualmente connesse al Router.

Active PC in LAN	
IP Address	MAC Address
☐ 192.168.1.206	02:11:85:c4:22:ba
☐ 192.168.1.207	02:11:85:c4:22:d1

Selezionare la periferica che si desidera filtrare o permettere e premere il tasto **Add** per copiare i MAC Address all'interno della Mac Address List.

7.1.5 Wireless

In questa sezione è possibile impostare tutti i parametri relative all'interfaccia wireless. E' altresì possibile configurare fino a 4 link WDS (Wireless Distribution System) al fine di stabilire connessioni tra 2 o più Access Point. Per la configurazione di un link WDS, è necessario conoscere l'indirizzo MAC dell'Access Point al quale si desidera connettere il WebShare Router.

La tecnologia WDS (Wireless Distribution System) non è sottoposta ad alcun standard specifico ed è sviluppata in maniera proprietaria dai vari produttori di chipset radio. Per queste motivazioni, connessioni

WDS tra apparati differenti potrebbero presentare comportamenti anomali, fino alla mancata realizzazione della connessione tra gli stessi.

Wireless	
Parameters	
WLAN Service	(•) Enable ( ) Disable
Mode	802.11b + g + n
ESSID	A02-RAU244-W300N
ESSID Broadcast	(•) Enable ( ) Disable
Regulation Domain	Europe
Channel Width	40/20 MHz
Channel ID	Channel 6 (2.437 GHz)
Tx PowerLevel	100 (Range: 1 ~ 100, unit in percentage)
Connected	true
AP MAC address	00:04:ed:42:ef:da
AP Firmware Version	1.1.7.0
WMM	( ) Enable (•) Disable
Wireless Distribution System (WDS)	
WDS Service	(•) Enable ( ) Disable
Peer WDS MAC address	1. 00:18:e7:53:8b:a6 2. 3. 4.

Parameters

Campo	Descrizione
WLAN Service	Abilita o disabilita il modulo radio integrato.
Mode	Selezionare la modalità di connessione tra le scelte proposte. Al fine di garantire un elevato grado di compatibilità con la maggior parte dei client, si consiglia di mantenere l'impostazione di default **802.11b + g + n**.
ESSID	Inserire il nome identificativo da assegnare alla rete wireless.

ESSID Broadcast	ESSID Broadcast è una funzione che permette di attivare/disattivare l'invio a tutti i client che ne facessero richiesta del valore ESSID identificativo della rete. Selezionare **Enable** per permettere che la rete venga visualizzata dai client durante le scansioni di ricerca, oppure **Disable** per rendere non visibile l'identificativo della rete.
Regulation Domain	Indicare la regione di utilizzo del prodotto (Atlantis Land ricorda che l'utilizzatore che viola tale impostazione è consapevole di poter infrangere la legislazione locale).
Channel Widht	Selezionare l'ampiezza di banda del canale di trasmissione.
Channel ID	Selezionare il canale da utilizzare per la trasmissione radio.
TX Power Level	Indica la percenutale (calcolata sulla Potenza massima emettibile) di potenza all'emettitore del modulo radio.
Connected	Indica lo stato della connessione tra il modulo Mini-PCI integrato e il sistema.
AP Mac Address	Indica l'indirizzo MAC associato all'interfaccia radio del prodotto.
AP Firmware Version	Indica la versione di firmware attualmente utilizzata per la gestione della parte wireless.
WMM	Abilita o disattiva il supporto Wi-Fi Multimedia per la gestione della qualità del servizio dei flussi multimediali su reti wireless.

WDS – Wireless Distribution System

Field	Description
WDS Service	Abilita o disabilita la funzionalità Wireless Distribution System.
Peer WDS MAC Address (1-4)	Indicare gli indirizzi MAC degli Access Poin/Router con supporto WDS con I quail si intende stabilire un link diretto.

- Il campo ESSID è case sensitive e non può superare il limite massimo di 32 caratteri ASCII.
- Atlantis Land consiglia la selezione di un canale non occupato, in quanto eventuali sovrapposizioni spaziali, temporali e di frequenza potrebbero indurre drastici cali in termini di performance.
- Nel campo MAC Address, si ricorda che gli indirizzi devono contenere il carattere separatore (:)

7.1.6 Wireless Security

In questa sezione è possibile attivare un profile di crittografia al fine di proteggere la WLAN da accessi non desiderati. Il prodotto supporta i più avanzati criteri di protezione attualmente disponibili garantendo alcuna degradazione in termini di performance della rete wireless.
Di seguito sono riportate le configurazioni disponibili:

WEP (Wired Equivalent Privacy)

Security Parameters

Parametro	Descrizione
Security Mode	Selezionare l'opzione **WEP**.
WEP Authentication	Selezionare la modalità di autenticazione tra **Open System** o **Shared Key** (la stessa condizione dovrà essere riportata sui

	client wireless).
WEP Encryption	Selezionare la lunghezza della chiave crittografica (64 o 128 bit) da utilizzare per la cifratura del traffico e la modalità di immissione della stessa (**Hex** o **ASCII**).
Passphrase (attivo solo in caso di selezione della modalità HEX)	Inserire la parola da utilizzare per la generazione delle 4 chiavi crittografiche e premere il tasto **Generate**; il sistema in automatico provvederà a creare 4 chiavi WEP della lunghezza selezionata (8 o 13 caratteri) ed all'immissone delle stesse nei campi **Key 1-4**. **NB: In questo caso le chiavi non andranno reinserite manualmente nei campi Key 1-4.**
Default Used WEP Key	Selezionare la chiave da utilizzare correntemente tra le 4 disponibili.
Key 1 – 4	Inserire le chiavi da utilizzare per la crittografia dei dati nel formato selezionato nel campo Wep Encryption (5 coppie esadecimali o caratteri ASCII nel caso di 64bit oppure 13 nel caso di 128 bit).

WPA-PSK (Wi-Fi Protected Access)

Security Parameters

Parametro	Descrizione
Security Mode	Selezionare l'opzione **WPA-PSK**.
WPA Shared Key	Inserire la chiave da utilizzare per la fase di autenticazione e crittografia dei dati.
Group Key Renewal	Inserire l'intervallo di tempo (espresso in secondi) al termine del quale verrà rinegoziata la chiave di crittografia.

WPA2-PSK (Wi-Fi Protected Access)

Security Parameters

Parametro	Descrizione
Security Mode	Selezionare l'opzione **WPA2-PSK**.

Per tutti gli altri parametri, si prega di fare riferimento alle indicazioni riportate per l'algoritmo WPA-PSK.

Premere su **Apply** per confermare le impostazioni.

7.1.7 Wireless Client/MAC Address Filter

Questa sezione permette di configurare una policy di filtraggio basata sugli indirizzamento MAC dei dispositive collegati via wireless al Router al fine di inibire accessi non autorizzati alla rete LAN.
Le politiche di filtering attivabili si riassumono come segue:

- **Blocca tutto tranne ciò che viene esplicitamente dichiarato:** utilizzando questo metodo, il dispositivo bloccherà l'accesso a qualsiasi dispositivo non sia specificatamente dichiarato nella MAC Address List.
- **Permettere tutto tranne ciò che viene esplicitamente dichiarato:** in questo caso, il prodotto permetterà l'accesso a qualsiasi dispositivo non sia specificatamente dichiarato nella MAC Address List.

Il prodotto supporta fino a 16 regole di filtraggio (non è configurato alcun preset di fabbrica) configurabili come segue:

Parametro	Descrizione
Filter Action	Selezionare la policy tra le seguenti: • **Disable:** la funzionalità non è abilitata • **Allowed:** In questo caso, il dispositivo negherà

	l'accesso alla rete a tutti i dispositivi non specificatamente riportati nel campo MAC Address List. • **Blocked:** In questo caso, il dispositivo permettà l'accesso alla rete a tutti i dispositivi non specificatamente riportati nel campo MAC Address List, bloccando quelli presenti nel campo MAC Address List.
Mac Address List	Impostare gli indirizzi MAC che si desidera bloccare o permettere, in relazione alla tipologia di filtraggio precedentemente selezionata.

Al fine di facilitare l'inserimento degli indirizzamenti MAC da filtrare, premendo il tasto Candidates ▸ sarà possibile visualizzare una lista delle periferiche attualmente connesse al Router tramite wireless.

Active PC in LAN	
IP Address	MAC Address
☐ 192.168.1.206	02:11:85:c4:22:ba
☐ 192.168.1.207	02:11:85:c4:22:d1

Selezionare la periferica che si desidera filtrare o permettere e premere il tasto **Add** per copiare i MAC Address all'interno della Mac Address List.

7.1.8 WPS

Il prodotto supporta pienamente le specifiche Wi-Fi Protected Setup, al fine di consentire una semplice installazione della rete wireless.
Questo insieme di specifiche prevede che le fasi di sincronizzazione e messa in sicurezza della WLAN vengano gestite in maniera autonoma dai dispositivi che supportino tali funzionalità.
Nello specifico, WPS prevede 2 modalità di sincronizzazione tra il punto di accesso ed i relativi client: la prima prevede la pressione di un apposito pulsante sul punto di accesso e successivamente su tutti i client appartenenti alla stessa wireless network. Questa procedura avvierà un processo di sincronizzazione automatica durante il quale i

prodotti, oltre che all'autenticazione presso il punto di accesso, negozieranno una chiave di sicurezza (secondo gli standard supportati dai vari client) per la messa in sicurezza della rete. Al termine della procedura la rete wireless sarà così configurata e pronta per essere utilizzata.
La seconda prevede che la fase di autenticazione dei client sul punto di accesso avvenga tramite il riconoscimento di un codice PIN univoco associato al client, mentre tutta la parte successiva di messa in sicurezza sarà identica alla modalità illustrata sopra. Esistono 2 modalità di autenticazione (Enrollee o Registar) in base al dispositivo che si occuperà di gestire la fase iniziale di autenticazione.
Nello specifico, vediamo ora come configurare le 2 modalità di associazione WPS sul WebShare 3G 244WN.

WPS Button Setup

1. Premere il pulsante WPS posto sulla parte posteriore del WebShare Router; il led Wireless comincerà a lampeggiare in maniera regolare.

2. Premere il pulsante WPS sul client o sui client che si desidera far autenticare al WebShare Router entro 120 secondi.

In alcune tipologie di client, il pulsante WPS può non essere presente; si prega di consultare il manuale utente per la verifica del supporto di questa tecnologia e per l'eventuale modalità di attivazione.

WPS PIN Setup (Enrollee o Registar Mode)

1. Identificare il codice WPS PIN sul client wireless che si desidera associare al prodotto.

2. Accedere alla sezione WPS del WebShare Router ed impostare i parametri come da figura:

3. Inserire il PIN rilevato secondo le modalità indicate al punto uno nel campo **Enrollee's PIN**.
4. Accedere alla configurazione del client wireless ed impostare il PIN indicato nel campo **WPS PIN** come codice per l'autenticazione del punto di accesso.

7.1.9 Port Setting

Questa sezione permette la configurazione dei parametri relative alle porte Gigabit Ethernet integrate nel dispositivo, quail modalità di trasmissione, velocità e supporto delle modalità di QoS avanzato basato su Protocollo IP.

Parametro	Descrizione
Port # Connection Type	Impostare la velocità (10/100/1000Mbps) e la modalità di trasmissione (Half/Full-Duplex) della porta LAN. Nel caso in cui non si conoscano le configurazioni della scheda di rete, è consigliato mantenere il parametro Auto. Per disattivare la porta LAN, selezionare la voce Disable.
IPv4 TOS Priority Control	Permette di impostare la modalità di prioritizzazione del traffico ToS. Questa funzionalità permette al prodotto di verificare il campo ToS contenuto nei pacchetti IP e classificarli in base al livello di priorità in modo da poter attuare policy di QoS avanzate.

7.1.10 DHCP Server

WebShare 3G 244WN dispone di un server DHCP integrato per la gestione dell'assegnazione degli indirizzi IP all'interno della LAN. In questa sezione viene riportato come configurare questo servizio.

Parametro	Descrizione
DHCP Server Mode	Selezionare una tra le modalità descritte: • **Disable:** disabilita il servizio DHCP Server; in questo modo, ogni macchina presente all'interno della rete dovrà impostare in maniera statica sulla scheda di rete un indirizzamento IP congruente a quello impostato sull'interfaccia LAN del Router. • **DHCP Server:** abilita la funzionalità DHCP Server e permette la configurazione dei parametri relativi, quale pool di assegnazione, tempo di lease, etc. • **DHCP Relay Agent:** permette al Router di collettare le richieste DHCP proveniente dai client a lui collegate ed indirizzarle verso un server DHCP presente sulla rete (Server, etc); in questo modalità, non sarà il Router ad occuparsi dell'assegnazione degli indirizzi IP ma un server esterno al prodotto.

Abilitando la funzione DHCP Server, sarà possibile configurare alcuni parametri per la gestione avanzata del servizio (di seguito si riporta una breve descrizione dei parametri principali). Si consiglia la modifica di queste impostazioni solo ad utenti esperti.

Parametro	Descrizione

Allow Bootp	Abilita l'assegnazione di un indirizzo IP da parte del DHCP Server anche ai client che utilizzano il protocollo BootP (Bootstrap protocol).
Allow Unknown Clients	Se abilitato, il DHCP server rilascerà un indirizzo IP a tutti i client che ne facciano richiesta.
Use Default Range	Se abilitato, imposta in maniera automatica il range di assegnazione del DHCP Server, utilizzando i primi 20 indirizzi IP appartenti alla stessa subnet dell'interfaccia LAN.
Starting IP Addres	Inserire l'indirizzo di partenza per la definizione del pool di assegnazione DHCP.
Ending IP Address	Inserire l'indirizzo finale per la definizione del pool di assegnazione DHCP.
Default Lease Time	Indica l'intervallo al termine del quale un associazione DHCP verrà ritenuta scaduta e quindi necessiterà di un rinnovo.
Use Router as DNS Server	Abilita la funzionalità DNS Server integrata. In questa modalità, le richieste DNS generate dai client verranno inoltrate al Router che provvederà alla risoluzione delle stesse.
Primary DNS Server Address	Indicare l'indirizzo del server DNS primario che verrà assegnato ai client che effettueranno una richiesta DHCP.
Secondary DNS Server Address	Indicare l'indirizzo del server DNS primario che verrà assegnato ai client che effettueranno una richiesta DHCP.
Use Router as Default Gateway	Spuntare questa opzioni se si desideri che il Router diventi il gatewat predefinito dei client impostati in DHCP mode.

Sarà inoltre possibile configurare delle associazioni fisse per esigenze particolari (es: Server di rete). Per attivare tale funzionalità, selezionare l'opzione **Fixed Host** ed operare come segue:

Fixed Host

Name	IP Address	MAC Address	Maximum Lease Time
		00:00:00:00:00:00	

Add Edit / Delete *(MAC Address Format is 'xx:xx:xx:xx:xx:xx')*

Edit	Name	IP Address	MAC Address	Maximum Lease Time	Delete

Parametro	Descrizione
Name	Inserire il nome dell' host che si intende associare in maniera statica.
IP Address	Indicare l'indirizzo IP che si intende associare al client.
MAC Address	Indicare l'indirizzamento MAC del client che si desidera sottoporre a questa associazione statica.
Maximum Lease Time	Impostare il tempo di validità relativamente all'associazione in oggetto.

Sarà inoltre possibile impostare il WebShare 3G 244WN in modalità DHCP Relay Agent, indicando l'indirizzo della macchina che si occuperà di gestire le richieste DHCP dei client collegati al prodotto.

DHCP
DHCP Relay Agent
DHCP Server IP Address 192.168.1.100
Apply

7.2 WAN – Wide Area Network

Questa sezione permette la configurazioni dei parametri relativi all'interfaccia WAN (ADSL2+/3G) del WebShare 3G 244WN.

7.2.1 WAN Interface

Le impostazioni di fabbrica dell'interfaccia WAN sono di seguito riportate:

Profilo WAN	
Encapsultation	PPPoA
Multiplexing	VC-Mux
Mode	Routing
VPI/VCI	8/35

E' possibile configurare l'interfaccia WAN secondo differenti modalità operative (ADSL, 3G oppure ADSL WAN Backup).

Single WAN ADSL

In questa tipologia di connessione, l'interfaccia ADSL viene utilizzata come connessione primaria e non sono attive le funzionalità di backup. Si prega di fare riferimento al paragrafo 6.1 per ulteriori approfondimenti.

Single WAN 3G

In questa tipologia di connessione, l'interfaccia 3G/UMTS viene utilizzata come connessione primaria e non sono attive le funzionalità di backup. Si prega di fare riferimento al paragrafo 6.2 per ulteriori approfondimenti.

Dual WAN ADSL/3G con backup mode

In questa tipologia di connessione, l'interfaccia ADSL viene utilizzata come connessione primaria mentre l'interfaccia 3G viene attivata solo in caso di failover della prima. Con questa modalità è possibile quindi effettuare un backup della connessione in caso di disservizi di natura tecnica sulla linea ADSL, cosi da fornire una connessione sempre attiva. Grazie all'evoluta gestione della modalità WAN backup, WebShare 3G 244WN è in grado di stabilire in maniera autonoma il failback della connessione ADSL e di attivare la connessione 3G opzionale per il backup della connettività. Al momento del ripristino della connessione sulla linea principale, il prodotto provvederà a switchare dalla linea di backup a quella primaria, gestendo in maniera completamente automatica tutte le procedure di failback.

Attenzione: L'utilizzo del WebShare 3G 244WN non è consigliato con abbonamenti con tariffazione basata sul tempo di connessione/traffico.

Il modem 3G non è incluso nell'offerta ed andrà acquistato separatamente. Si prega di verificare la compatibilità del modem acquistato tramite la lista presente al termine di questo manuale o reperibile sul sito www.atlantis-land.com presso la sezione dedicata al prodotto.

La configurazione dell'interfaccia 3G può avvenire anche senza che il modem 3G sia fisicamente collegato al prodotto.

Di seguito è indicato come configurare i parametri per utilizzare questa modalità di connessione:

WAN Interface	
WAN Interface	
Main Port	ADSL (Current Main Port: 3G)
Failover Parameters	
Failover / Failback	☑ Enable
Backup Port	3G (Connection will be set always on.)
Keep Backup Interface Connected	☐ Enable
Connectivity Decision	Not in service when probing failed after 5 consecutive times.
Failover Probe Cycle	Every 12 seconds
Failback Probe Cycle	Every 3 seconds
Detect Rule (either one)	1. ADSL Down 2. Ping Fail ○ No Ping ○ Ping Gateway ◉ Ping Host 151.91.125.3
Apply	

WAN Interface

Parametro	Descrizione
Main Port	Permette di scegliere l'interfaccia WAN da utilizzare come connessione primaria. Selezionare **ADSL**.

Failover Parameters

Parametro	Descrizione
Failover/Failback	Spuntare l'opzione per attivare la modalità di gestione del failover/failback per la connessione primaria (ADSL).
Backup Port	Indica l'interfaccia WAN utilizzata per le attività di backup della connessione.
Keep Backup Interface Connected	Selezionare questa opzione per mantenere attiva la connessione di backup anche al ripristino della connessione primaria **Questa opzione non è consigliata nel caso di abbonamenti con tariffazione a tempo/pacchetti**.

Connectivity Decision	Impostare il numero di cicli di diagnostica falliti necessari affinchè il prodotto costruisca la connessione sull'interfaccia di backup.
Failover Probe Cycle	Impostare l'intervallo di durata del ciclo di diagnostica per il rilevamento del failover dell'interfaccia ADSL.
Failback Probe Cycle	Impostare l'intervallo di durata del ciclo di diagnostica per il rilevamento del failback dell'interfaccia ADSL.
Detect Rule	Selezionare attraverso quale modalità il Router effettuerà la diagnostica del corretto funzionamento della connessione primaria. Sono disponibili 4 differenti opzioni: • **ADSL Down:** Questa opzione non è deselezionabile e permette al Router di attivare la connessione backup nel momento in cui rilevi una disconnessione elettrica (disallineamento della portante) sull'interfaccia ADSL. • **Ping Fail:** Questa opzione permette di attivare la connessione backup al fallimento di una richiesta di Echo. Selezionare **No Ping** per non attivare questa modalità di rilevamento, **Ping Gateway** nel caso in cui si desideri che all'avvio di ogni Probe Cycle il Router invii una richiesta ECHO al Default Gateway oppure **Ping Host** per far si che la richiesta echo venga indirizzata verso un host esterno dichiarato dall'utente anziché verso il Gateway.

I parametri impostati all'interno dei campi **Failover Probe Cycle** e **Failback Probe Cycle** indicano ogni quanto vengono eseguiti i test diagnostici per il rilevamento del failover o failback della connessione ADSL.

La condizione necessaria per l'attivazione della connessione di backup è dovuta al numero di fallimenti indicati nel campo **Connectivity Decision** moltiplicati per l'intervallo impostato nel campo **Failover Probe Cycle**.

Ad esempio, impostando il campo **Connectivity Decision** con valore

5 ed il campo **Failover Probe Cycle** con valore 6, in caso di caduta della connessione ADSL, la connessione di backup verrà attivata dopo 6 secondi x 5 volte = 30 secondi dal primo test diagnostico fallito.

Premere **Apply** per confermare.

A questo punto sarà necessario configurare i dati per la connessione ADSL e 3G tramite la sezione **WAN Profile**.

7.2.2 WAN Profile

In questa sezione è possibile configurare i profili di connessione sia per ll'interfaccie ADSL che quella 3G. Si ricorda che il prodotto è in grado di supportare più profili PVC sull'interfaccia ADSL per la veicolazione di servizi differenti (dati, fonia, IPTV).

Si ricorda che nel caso in cui sia stata attivata la modalità di backup ADSL over UMTS, dovranno essere configurate entrambe le interfaccie. Utilizzare il campo **Profile Port** per navigare attraverso le interfaccie e configurare il profilo ADSL e quelo UTMS.

Si ricorda che tale dispositivo non è adatto a gestire abbonamenti non FLAT (a consumo). Atlantis Land non potrà essere ritenuta responsabile per qualsiai problematica derivante dall'utilizzo di abbonamenti a consumo (non FLAT) o da una errata configurazione dell'apparato.
In caso di dubbio contattare, prima di effettuare la configurazione del dispositivo, l'assistenza tecnica.

Di seguito sono riportate per comodità le configurazioni possibili sia per l'interfaccia ADSL che per quella 3G:

ADSL - PPPoE Connection

PPPoE (PPP over Ethernet) è una connessione ADSL conosciuta come dial-up DSL. Al pari del PPPoA e' stata concepita per integrare servizi a banda larga con un'attenzione particolare alla facilità di configurazione. L'utente può beneficiare di una grande velocità di accesso senza cambiare l'idea di funzionamento e condividere lo stesso account con l'ISP. Non è richiesto alcun software aggiuntivo.

Parametro	Descrizione
Profile Port	Selezionare la porta a cui applicare il profilo di connessione.
Protocol	Selezionare il protocollo ATM da utilizzare.
Description	Inserire un nome identificativo per il profilo di connessione.
VPI/VCI	Inserire i valori di VPI e VCI forniti dal provider.
ATM Class	Selezionare il valore di Quality of Server per la tratta ATM.
Username	Fornita dall'ISP, tale username può essere composta da massimo 63 caratteri (case sensitive) alfanumerici.
Password	Fornita dall'ISP, tale password può essere composta da massimo 63 caratteri (case sensitive) alfanumerici.
Service Name	Lasciare vuoto se non espressamente comunicato dall'ISP. E' un identificativo, può essere richiesto da alcuni ISP. Al solito può

	essere composto da massimo 63 caratteri (case sensitive) alfanumerici.
NAT	Scegliere disable solo in caso si possieda una classe pubblica o se il prodotto viene fatto funzionare come Bridge.
IP	Lasciare 0.0.0.0 per ottenere automaticamente l'indirizo IP dall'ISP, in caso contrario inserire l'indirizzo IP fisso.
Auth. Protocol	Scegliendo l'opzione **Auto**, viene utilizzato prima il protocollo CHAP e poi, in caso di insuccesso, il PAP.
Connection	Scegliere **Always On** per mantenere attiva sempre la sessione PPPoE/PPPoA. Scegliere **Connect On-Demand** per far costruire la connessione solo in caso di traffico.
Idle Timeout	Il dispositivo disconnette automaticamente la connessione ADSL quando non rileva alcuna attività di pacchetti verso Internet per un tempo predeterminato. Il valore può essere settato in minuti, come default è 0. Lasciando 0 il Router non si disconnetterà mai.
MTU	Indica le dimensioni massime del datagramma transitante sull'interfaccia.
RIP	Scegliere il protocollo RIP da abilitare sull'interfaccia WAN.
TCP MSS Clamp	Se attivato, permette di gestire le trasmissioni TCP senza frammentazione, anche nel caso in cui il frame sia maggiore del valore impostato nel campo MTU.
MAC Spoofing	Se abilitato, permette di impostare un indirizzamento MAC definito dall'utente associandolo all'interfaccia WAN.
Obtain DNS	Selezionare **Automatic** se si desidera che gli indirizzi DNS vengano negoziati al momento della connessione PPP. Nel caso in cui si desideri impostare dei server DNS differenti, deselezionare questa opzione ed inserire gli indirizzi DNS nei campi **Primary** e **Secondary**.

Si ricorda che tale dispositivo non è adatto a gestire abbonamenti non FLAT (a consumo). Atlantis Land non potrà essere ritenuta responsabile per qualsiai problematica derivante dall'utilizzo di abbonamenti a consumo (non FLAT) o da una errata configurazione dell'apparato.

In caso di dubbio contattare, prima di effettuare la configurazione del dispositivo, l'assistenza tecnica.

ADSL - PPPoA Connection

Parametro	Descrizione
Profile Port	Selezionare la porta a cui applicare il profilo di connessione.
Protocol	Selezionare il protocollo ATM da utilizzare.
Description	Inserire un nome identificativo per il profilo di connessione.
VPI/VCI	Inserire i valori di VPI e VCI forniti dal provider.
ATM Class	Selezionare il valore di Quality of Server per la tratta ATM.
Username	Fornita dall'ISP, tale username può essere composta da massimo 63 caratteri (case sensitive) alfanumerici.
Password	Fornita dall'ISP, tale password può essere composta da massimo 63 caratteri (case sensitive) alfanumerici.
Service Name	Lasciare vuoto se non espressamente comunicato dall'ISP. E' un identificativo, può essere richiesto da alcuni ISP. Al solito può essere composto da massimo 63 caratteri (case sensitive) alfanumerici.
NAT	Scegliere disable solo in caso si possieda una classe pubblica o se il prodotto viene fatto funzionare come Bridge.
IP	Lasciare 0.0.0.0 per ottenere automaticamente l'indirizo IP dall'ISP, in caso contrario inserire l'indirizzo IP fisso.

Auth. Protocol	Scegliendo l'opzione **Auto**, viene utilizzato prima il protocollo CHAP e poi, in caso di insuccesso, il PAP.
Connection	Scegliere **Always On** per mantenere attiva sempre la sessione PPPoE/PPPoA. Scegliere **Connect On-Demand** per far costruire la connessione solo in caso di traffico.
Idle Timeout	Il dispositivo disconnette automaticamente la connessione ADSL quando non rileva alcuna attività di pacchetti verso Internet per un tempo predeterminato. Il valore può essere settato in minuti, come default è 0. Lasciando 0 il Router non si disconnetterà mai.
MTU	Indica le dimensioni massime del datagramma transitante sull'interfaccia.
RIP	Scegliere il protocollo RIP da abilitare sull'interfaccia WAN.
TCP MSS Clamp	Se attivato, permette di gestire le trasmissioni TCP senza frammentazione, anche nel caso in cui il frame sia maggiore del valore impostato nel campo MTU.
MAC Spoofing	Se abilitato, permette di impostare un indirizzamento MAC definito dall'utente associandolo all'interfaccia WAN.
Obtain DNS	Selezionare **Automatic** se si desidera che gli indirizzi DNS vengano negoziati al momento della connessione PPP. Nel caso in cui si desideri impostare dei server DNS differenti, deselezionare questa opzione ed inserire gli indirizzi DNS nei campi **Primary** e **Secondary**.

Premere il pulsante Edit/Delete per applicare le modifiche.

Si ricorda che tale dispositivo non è adatto a gestire abbonamenti non FLAT (a consumo). Atlantis Land non potrà essere ritenuta responsabile per qualsiai problematica derivante dall'utilizzo di abbonamenti a consumo (non FLAT) o da una errata configurazione dell'apparato.

In caso di dubbio contattare, prima di effettuare la configurazione del dispositivo, l'assistenza tecnica.

ADSL - MPoA Connection (RFC 1483)

Parametro	Descrizione
Profile Port	Selezionare la porta a cui applicare il profilo di connessione.
Protocol	Selezionare il protocollo ATM da utilizzare.
Description	Inserire un nome identificativo per il profilo di connessione.
VPI/VCI	Inserire i valori di VPI e VCI forniti dal provider.
ATM Class	Selezionare il valore di Quality of Server per la tratta ATM.
NAT	Scegliere disable solo in caso si possieda una classe pubblica o se il prodotto viene fatto funzionare come Bridge.
IP	Inserire l'indirizzo IP fisso fornito dal provider.
Netmask	Inserire la maschera di rete relativa all'indirizzo IP impostato nel campo IP.
Gateway	Inserire l'indirizzo Gateway per l'instadamento del traffico WAN verso Internet.
RIP	Scegliere il protocollo RIP da abilitare sull'interfaccia WAN.
TCP MSS Clamp	Se attivato, permette di impostare il miglior valore MTU in maniera automatica.
MAC Spoofing	Se abilitato, permette di impostare un indirizzamento MAC

	definito dall'utente associandolo all'interfaccia WAN.
Obtain DNS	Selezionare **Automatic** se si desidera che gli indirizzi DNS vengano negoziati al momento della connessione PPP. Nel caso in cui si desideri impostare dei server DNS differenti, deselezionare questa opzione ed inserire gli indirizzi DNS nei campi **Primary** e **Secondary**.

ADSL - IPoA Routed Connection (RFC 1577 Routed)

Parametro	Descrizione
Profile Port	Selezionare la porta a cui applicare il profilo di connessione.
Protocol	Selezionare il protocollo ATM da utilizzare.
Description	Inserire un nome identificativo per il profilo di connessione.
VPI/VCI	Inserire i valori di VPI e VCI forniti dal provider.
ATM Class	Selezionare il valore di Quality of Server per la tratta ATM.
NAT	Scegliere disable solo in caso si possieda una classe pubblica o se il prodotto viene fatto funzionare come Bridge.
IP	Inserire l'indirizzo IP fisso fornito dal provider.
Netmask	Inserire la maschera di rete relativa all'indirizzo IP impostato nel campo IP.
Gateway	Inserire l'indirizzo Gateway per l'instadamento del traffico WAN verso Internet.
RIP	Scegliere il protocollo RIP da abilitare sull'interfaccia WAN.
TCP MSS Clamp	Se attivato, permette di impostare il miglior valore MTU in maniera automatica.
MAC Spoofing	Se abilitato, permette di impostare un indirizzamento MAC definito dall'utente associandolo all'interfaccia WAN.
Obtain DNS	Selezionare **Automatic** se si desidera che gli indirizzi DNS

	vengano negoziati al momento della connessione PPP. Nel caso in cui si desideri impostare dei server DNS differenti, deselezionare questa opzione ed inserire gli indirizzi DNS nei campi **Primary** e **Secondary**.

Si ricorda che in questa modalità è necessario configurare i PC con i DNS (al Router non vengono passati dall'ISP). Nel caso di un singolo indirizzo IP pubblico lasciare il NAT su Enable.

Le principali modalità in cui l'ISP può fornire RFC1483/RFC1577 possono essere diverse:

- **Un indirizzo IP pubblico statico.** In questo caso bisognerà settare la sezione Configuration-Wan nella seguente modalità: **Static IP address**=IP statico pubblico assegnato dall'ISP, **Subnet mask** e **Default Gateway** (che sarà un IP pubblico) che sono fornite dal provider. In Configuration-Lan impostare il Lan-IP in una classe privata che sarà il default gateway di tutti i PC (se non si attiva il DHCP). **Abilitare il NAT**. E' opportuno dare a tutti i PC i server DNS.
- **Una classe di IP statici con Punto-Punto pubblica.** In questo caso bisognerà settare la sezione Configuration-Wan nella seguente modalità: **Static IP address** =IP statico pubblico assegnato dall'ISP (quello della punto-punto), **Subnet mask** e **Default Gateway** (che sarà un IP pubblico) che sono fornite dal provider. In Configuration-Lan impostare il Lan-IP sull'IP statico pubblico (che fa parte della classe assegnata dall'ISP) con la rispettiva subnet mask. Gli altri IP di questa classe (e la subnet mask) dovranno essere messi sui PC assieme al default gateway che sarà il Lan-IP dell' Adsl2+ Router (è opportuno mettere i DNS). **Disabilitare il NAT**.
- **Una classe di IP statici con Punto-Punto privata.** In questo caso bisognerà settare la sezione Configuration-Wan nella seguente modalità: **Static IP address** =IP statico privato assegnato (quello della punto-punto) dall'ISP, **Subnet mask** e **Default Gateway** (che sarà un

IP privato) che sono fornite dal provider. In Configuration-Lan impostare il Lan-IP sull'IP statico pubblico (che fa parte della classe assegnata dall’ISP) con la rispettiva subnet mask. Gli altri IP di questa classe (e la subnet mask) dovranno essere messi sui PC assieme al default gateway che sarà il Lan-IP dell’ Adsl2+ Router (è opportuno mettere i DNS). **Disabilitare il NAT**.

ADSL - Pure Bridge

Per particolari applicazioni può essere necessario configurare il Router come un Bridge. In questo modo l'indirizzo IP assegnato dal provider verrà girato al PC che pertanto potrà far girare particolari applicazioni non trasparenti al NAT. Tale configurazione è valida in caso di PPPoE.

Parametro	Descrizione
Profile Port	Selezionare la porta a cui applicare il profilo di connessione.
Protocol	Selezionare il protocollo ATM da utilizzare.
Description	Inserire un nome identificativo per il profilo di connessione.
VPI/VCI	Inserire i valori di VPI e VCI forniti dal provider.
ATM Class	Selezionare il valore di Quality of Server per la tratta ATM.
Encap Method	Selezionare il metodo di incapsulazione tra LLc Bridge and Vc-Mux bridged.
Acceptable Frame Type	Specificare la tipologia di traffico transitante attraverso l'interfaccia WAN (tutto o solo traffico VLAN taggato).
Filter Type	Specificare il tipo di filtro effettuato dall'interfaccia bridge: • **All:** Permette il passaggio di tutti i pacchetti Ethernet attraverso l'interfaccia. • **IP:** Permette il solo passaggio di pacchetti Ethernet di tipo IP/ARP. • **PPPoE:** Permette il passaggio dei soli pacchetti Ethernet di tipo PPPoE attraverso l'interfaccia.

3G (configurazione generica valida per tutti gli operatori nazionali)

Parameters	
Profile Port	3G
iBurst	☐ Enable
Mode	UMTS first
TEL No.	*99***1#
APN	internet
Username	
Password	
Auth. Protocol	Chap(Auto)
MTU	1500
PIN	
Connection	Always On
Keep Alive	☐ Enable
Obtain DNS automatically	☑ Enable
Primary DNS/Secondary DNS	0.0.0.0 / 0.0.0.0

*Warning: Entering the wrong PIN code three times will lock the SIM.

Apply

Connection

Parametro	Descrizione
Profile Port	Indica l'interfaccia di connessione 3G.
iBurst	Abilita la modalità di configurazione per i client wireless iBurst.
Mode	Permette la selezione dello standard di connessione 3G. E' possibile selezionare una tra le seguenti opzioni: • **Automatic:** Il Router provvede a stabile una connessione con lo standard in grado di fornire le migliori prestazioni (UTMS, GPRS o GSM) • **UMTS First:** viene privilegiata la connessione

	secondo standard HDSPA o HSUPA. Nel caso in cui non fosse possibile stabilire una connessione secondo questi standard, verranno percorsi differenti metodologie di connessione (GPRS/EDGE). • **GPRS/EDGE First:** viene privilegiata la connessione secondo standard GPRS/EDGE. • **UMTS Only:** La connessione viene stabilita esclusivamente attraverso rete UMTS. • **GSM Only:** La connessione viente stabilita esclusivamente su rete GSM (limitazioni di velocità di 9600bps).
Tel No.	Specificare il numero di telefono necessario per la connessione (GSM) oppure la stringa di inizializzazione per connessione 2G/3G. Il valore preimpostato *99***1# è il valore standard utilizzato da tutti gli operatori mobili italiani.
APN	Specificare l'APN fornito dall'ISP da utilizzare per la connessione 3G. Di seguito sono riportati i dati relativi ai maggiori operatori di telefonia mobile nazionali: • **APN TIM:** ibox.tim.it • **APN Vodafone:** web.omnitel.it • **APN WIND:** internet.wind • **APN WIND Business:** internet.wind.biz • **APN H3G (Sim ricaricabile):** tre.it • **APN H3G (Sim Dati):** datacard.tre.it
Username	Inserire il nome utente da utilizzare per l'autenticazione (solo se richiesto).
Password	Inserire la password da utilizzare per l'autenticazione (solo se richiesto).
Authentication Protocol	Selezionare il protocollo di autenticazione del profilo (non modificare se non espressamente richiesto).
MTU	Inserire il valore di Maximum Transfert Unit per connessione in oggetto.
PIN	Inserire l'eventuale codice PIN di sicurezza per la SIM card utilizzata. Si consiglia di utilizzare schede SIM senza la protezione PIN; in

	questo caso, lasciare vuoto il campo PIN.
Connection	Selezionare la tipologia di connessione.
Keep Alive	Se spuntato permette di mantenere attiva la connessione 3G anche al ripristino della connessione ADSL primaria. **Questa opzione non è consigliata nel caso di abbonamenti con tariffazione a tempo/pacchetti**.
Obtain DNS automatically	Spuntare l'opzione nel caso in cui si desideri che i server DNS vengano negoziati in maniera automatica al momento della connessione.
Primary DNS / Secondary DNS	Inserire i valori dei server DNS primario e secondario.

Attenzione: L'utilizzo del WebShare 3G 244WN non è consigliato con abbonamenti con tariffazione basata sul tempo di connessione/traffico.

Si consiglia di prestare la massima attenzione durante la configurazione dell'interfaccia 3G e di verificare le modalità di erogazione del servizio UMTS concordate con il proprio operatore di telefonia mobile.

7.2.3 ADSL Mode

In questa sezione è possibile configurare tutti i parametri relativi all'interfaccia ADSL. Si consiglia la modifica dei parametri contenuti in questa sezione solo nel caso in cui si rilevino particolari problematiche in termini di banda e/o stabilità della linea.

Parametro	Descrizione
Connect Mode	E' possibile selezionare la modalità **Auto** per avviare la procedura di auto discovery oppure selezionare manualmente la tipologia di linea ADSL utilizzata.
Modulation	Selezionare manualmente il tipo di modulazione utilizzato dalla linea ADSL nel caso di allineamento difficoltoso o su linee particolarmente rumorose.
Profile Type	Selezionare un profilo di connessione specifico nel caso in cui si verifichinoo problematiche di banda o di instabilità della connessione. Si consiglia la modifica di questo parametro solo nel caso di problematiche particolari e da parte di personale esperto.
Active Line	Impostare il parametro prima su **False** e successivamente su **True** per applicare le modifiche effettuate in questa schermata.
Coding Gain	Permette la regolazione della potenza trasmissiva del Router.

	Un valore di Coding Gain molto alto può incrementare il valore di downstream ma causare instabilità nel collegamento ADSL.
Tx Attenuation	Selezionare il guadagno di trasmissione ADSL.
Elapsed Time	Indica il tempo di attività trascorso dall'ultima sincronizzazione.

Laddove il LED ADSL fosse lampeggiante è opportuno forzare la modulazione. Nella combo-Box **Connect Mode** forzare la voce ADSL. Cliccare su **Apply** e poi su **Save config to Flash** per rendere permanenti i settaggi.
Se il provider fornisce un contratto ADSL e la modalità connect mode è impostata su ADSL2 o ADSL2+ l'allineamento potrebbe essere particolarmente lungo e difficoltoso.

7.3 System

7.3.1 Time Zone

Il Router non ha un orologio al suo interno, usa il protocollo SNTP per risolvere tale inconveniente.

Time Zone
Parameters
Time Zone — Enable / Disable
Time Zone List — By City / By Time Difference
Local Time Zone (+-GMT Time) — (GMT+01:00)Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna
SNTP Server IP Address — 1. carl.css.gov 2. india.colorado.edu 3. time.nist.gov 4. time-b.nist.gov
Daylight Saving — Enabled
Resync Period — 1440 min(s)
Apply Cancel

Parametro	Descrizione
Time Zone	Selezionare **Enable** per attivare la funzionalità.
Time Zone List	Selezionare il criterio di ordinamento e visualizzazione del campo **Local Time Zone**.
Local Time Zone	Selezionare dalla lista la Time Zone del paese di appartenenza.
SNTP Server IP	Impostare i 4 server SNTP necessari per la sincronizzazione del

Address	client SNTP integrato.
DayLight Saving	Selezionare questa opzione per attivare l'ora legale.
ReSync Period	Inserire l'intervallo al termine del quale il client SNTP richiederà la successiva sincronizzazione con il server.

Per l'utilizzo della funzionalità Time Zone, è necessario verificare le seguenti condizioni:

- La connessione ad Internet (ADSL/3G) deve essere correttamente configurata e funzionante.
- Nel caso in cui i server DNS non siano correttamente impostati, potrebbe essere necessario sostituire i nomi dei server SNTP con i relativi indirizzi IP.

7.3.2 Remote Access

Attivando tale funzionalità è possibile attivare la configurazione remota dell'apparato via http:

Selezionando l'intervallo di tempo desiderato e cliccando su **Enable**, verrà concesso l'accesso alla configurazione del prodotto tramite l'IP pubblico. Di default la porta utilizzata è la 80, è comunque possibile modificare tale impostazione alla voce di menù **Device Management**.

Per rendere l'accesso remoto permanente è sufficiente creare nella sezione Virtual Server una regola apposita che ruoti la porta di configurazione sull'IP lato LAN del Router.

7.3.3 Firmware Upgrade

Per effettuare l'upgrade del firmware del dispositivo è necessario anzitutto scaricare dal sito **www.atlantis-land.com** (nella sezione opportuna) un nuovo firmware (se disponibile). Aprire il file compresso in una directory. Accedere a questo punto, sotto il menù **Configuration** e poi **System** , alla **voce Firmware Upgrade** e premere poi il tasto **Sfoglia** ed indicare la path contenente il firmware decompresso. Premere poi sul tasto **Upgrade** per terminare l'aggiornamento. E' opportuno staccare, durante la fase di upgrade, la linea ADSL dal dispositivo.

- E' opportuno garantire, durante l'intera fase di upgrade, al Router ADSL l'alimentazione elettrica. Qualora questa venisse a mancare il dispositivo potrebbe non essere recuperabile.
- Staccare il cavo RJ11 dal Router e verificare che solo un cavo ethernet sia connesso (quello del PC da cui si effetua l'upgrade).
- Effettuare l'upgrade utilizzando una connessione wired e non wireless. Questo potrebbe danneggiare il dispositivo ed invalidare così la garanzia.

- Non utilizzare file di restore generati con versioni anteriori di firmware. Questo potrebbe rendere instabile il dispositivo.
- Durante la procedura di upgrade è opportuno non chiudere il browser Web, caricare nuove pagine o cliccare su link. Questo potrebbe danneggiare il firmware e rendere inusabile il dispositivo.

Durante la fase di upgrade il Router indicherà lo stato di completamento della riscrittura del firmware mostrando un indicatore percentuale.
Completata la procedura apparirà una schermata in cui è possibile scegliere se mantenere gli attuali settaggi (**Current Settings**) o ripristinare il dispositivo alle condizioni iniziali (**Factory Default Settings**).

7.3.4 Backup / Restore

Il WebShare Router consente di effettuare un backup (ripristino) sul (dal) disco fisso del vostro PC. Grazie a questa comoda funzionalità è possibile salvare complesse configurazioni e rendere nuovamente operativo il Router in pochi veloci passaggi.

Per effettuare il Backup cliccare sul bottone **Backup**. Non resta che selezionare il percorso in cui salvare i dati sulla configurazione (verrà generato un file con estensione CFG).
Per effettuare il Ripristino cliccare sul bottone **Sfoglia**, indicando il percorso dove è contenuto il file contenente la configurazione, e cliccare poi su Restore.
La procedura è piuttosto lenta (il tempo complessivo può superare i 2 minuti) e termina con il riavvio del dispositivo.

Non editare per nessuna ragione il file di backup, questo potrebbe bloccare e rendere inutilizzabile il dipsositivo.

7.3.5 Restart Router

Se per necessità si desidera reimpostare il Router con la configurazione di default (perdendo tutti i settaggi inseriti) è sufficiente accedere, sotto il menù Configuration-System alla voce **Restart Router** e spuntare la voce **Factory Default Settings**. Premere poi il tasto **Restart Router**. Il Router effettuerà un reboot e caricherà i settaggi di default.
Premendo invece il tasto Restart con la scelta **Current Settings** il router effettuerà un reboot caricando la configurazione attuale.

7.3.6 User Management

Al fine di prevenire accessi non autorizzati all'interfaccia di configurazione del prodotto, è necessario garantire la possibilità di creazione di profile utente multipli, ciascuno protetto da password.
Tramite questa sezione è possibile modificare un account esistente oppure creare un nuovo profilo di accesso.
Per modificare un profilo esistente, selezionarlo tramite la spunta **Edit** come da figura:

Parametro	Descrizione
Valid	Indica la validità o la disattivazione dell'account selezionato.
User	Indica il nome utente da inserire in fase di accesso.
Comment	Inserire una descrizione per il profilo selezionato.
Password	Inserire la password da associare al profilo. Questa password andrà immessa, associata al nome utente, al momento dell'accesso all'interfaccia di configurazione del Router.
Confirm Password	Confermare la password inserita.

Sarà ora possibile salvare le modifiche apportate premendo il tasto **Edit/Delete** e poi **Save Config**.
Per eliminare un profilo esistente, selezionarlo tramite la spunta **Delete** e premere il tasto **Delete** per procedere con l'eliminazione come da figura:

Per aggiungere un nuovo profilo, immettere i dati necessari e premere il tasto **Add** come da figura:

7.4 Firewall and Access Control

Questa funzionalità offerta dal dispositivo è un firewall che consente una prima valida difesa nei confronti di qualche malintenzionato di cui Internet è piena. Le funzionalità offerte, pur essendo varie ed efficaci, non sono da ritenersi "sicure" sempre e comunque. Certamente potrebbero essere considerate ampiamente soddisfacenti in molte circostanze, ma data la varietà degli attacchi e la velocità con cui questi si evolvono, si consiglia sempre di non considerarsi inattaccabili. Qualora le informazioni

custodite siano particolarmente importanti consigliamo un'attenta configurazione del firewall e magari l'uso di prodotti, a supporto, più adatti al caso.

Il firewall presente all'interno del Router opera su 2 differenti livelli:

1. Anzitutto previene dagli accessi indesiderati dall'esterno della LAN. Questa operazione è articolata su 3 livelli:
    - **NAT:** quando abilitato (sempre, escluso in caso di classe pubblica) tutti i PC della LAN sono visti dall'esterno come un unico indirizzo IP. E' molto più difficile pertanto per un hacker accedere alla singola macchina.
    - **Packet Filter:** e' possibile filtrare per pacchetto e protocollo tutto quello che entra verso la LAN e far effettivamente passare solo il traffico ritenuto sicuro.
    - **Intrusion Detection:** questa sezione si occupa di effettuare una difesa attiva contro ogni tipo di attacco DoS. Ogni tentativo di attacco è memorizzato in un file di Log. Viene gestita inoltre una Balck List dinamica.

2. Previene inoltre gli accessi dalla LAN locale.
   - **Packet Filter:** e' possibile filtrare per pacchetto e protocollo tutto quello che esce verso Internet e far effettivamente passare solo il traffico ritenuto sicuro.
   - **Bridge Filtering(MAC):** consente l'accesso verso Internet di tutti e soli i MAC address desiderati (o ne impedisce l'accesso ad una lista).
   - **URL Filter:** permette di bloccare l'accesso a determinati siti.

E' consigliabile visitare periodicamente il sito di Atlantis Land (www.atlantis-land.com) al fine di reperire l'ultimo Firmware che potrebbe migliorare le caratteristiche del firewall.

7.4.1 General Settings

In questa sezione è possibile abilitare o disabilitare il modulo Firewall integrato e selezionare una tra le policy predefinite per la messa in sicurezza della rete.

Parametro	Descrizione
Security	Selezionare **Enable** per abilitare il firewall integrato.
Policy	• **All blocked/User-defined:** non è definito nulla. Tutto il traffico sia entrante che uscente è bloccato. L'utente deve configurare le proprie regole nella sezione Packet Filter. • **High/Medium/Low security level:** sono definiti tutta una serie di impostazioni preconfigurate modificabili che permettono un uso immediato. A seconda del grado di protezione scelto determinati servizi saranno o meno abilitati.
Block WAN Request	Se abilitata, inibisce le risposte alle richieste Echo (Ping) verso l'interfaccia WAN.

Di seguito sono riportate le preconfigurazioni del modulo Firewall in relazione al livello di sicurezza selezionato:

Predefined Port Filter

Application	Protocol	Port Number		Low Level		Medium Level		High Level	
		Start	End	Inbound	Outbound	Inbound	Outbound	Inbound	Outbound
HTTP(80)	TCP(6)	80	80	NO	YES	NO	YES	NO	YES
DNS (53)	UDP(17)	53	53	NO	YES	NO	YES	NO	YES
DNS (53)	TCP(6)	53	53	NO	YES	NO	YES	NO	YES

FTP(21)	TCP(6)	21	21	NO	YES	NO	YES	NO	NO
Telnet(23)	TCP(6)	23	23	NO	YES	NO	YES	NO	NO
SMTP(25)	TCP(6)	25	25	NO	YES	NO	YES	NO	YES
POP3(110)	TCP(6)	110	110	NO	YES	NO	YES	NO	YES
NEWS(NNTP) (Network News Transfer Protocol)	TCP(6)	119	119	NO	YES	NO	YES	NO	NO
RealAudio/ RealVideo (7070)	UDP(17)	7070	7070	YES	YES	YES	YES	NO	NO
PING	ICMP(1)	N/A	N/A	NO	YES	NO	YES	NO	YES
H.323(1720)	TCP(6)	1720	1720	YES	YES	NO	YES	NO	NO
T.120(1503)	TCP(6)	1503	1503	YES	YES	NO	YES	NO	NO
SSH(22)	TCP(6)	22	22	NO	YES	NO	YES	NO	NO

NTP /SNTP	UDP(17)	123	123	NO	YES	NO	YES	NO	YES
HTTP/HTTP Proxy (8080)	TCP(6)	8080	8080	NO	YES	NO	NO	NO	NO
HTTPS(443)	TCP(6)	443	443	NO	YES	NO	YES	N/A	N/A
ICQ (5190)	TCP(6)	5190	5190	YES	YES	N/A	N/A	N/A	N/A
MSN (1863)	TCP(6)	1863	1863	YES	YES	N/A	N/A	N/A	N/A
MSN (7001)	UDP(17)	7001	7001	YES	YES	N/A	N/A	N/A	N/A
MSN VEDIO (9000)	TCP(6)	9000	9000	NO	YES	N/A	N/A	N/A	N/A

Inbound: Internet to LAN ; **Outbound:** LAN to Internet; **YES:** Allowed ; **NO:** Blocked ; **N/A:** Not Applicable

Selezionando la policy All Blocked / User Defined, ogni regola dovrà essere creata manualmente dall'utente e non sarà possibile usufruire di alcuna regola preimpostata.

Si ricordi che tutto il traffico non contemplato nel set di regole viene scartato. E' comunque possibile aggiungere o modificare le regole al fine di ottenere un firewall che soddisfi particolari esigenze.
Ad esempio dopo aver scelto il firewall con impostazione di sicurezza **HIGH**, tra le altre cose il Router non risponderà ai Ping provenienti dall'esterno nè consentirà lo scaricamento via FTP di file dalla rete. Per modificare questa situazione è sufficiente accedere alla

sezione **Configuration - Firewall - Packet Filter**.

Sarà inoltre possibile abilitare le funzionalità SIP ALG e FTP ALG nel caso in cui si utilizzino dispositivo VoIP basati su standard SIP oppure servizi FTP.

Premere **Apply** per confermare le eventuali modifiche.

NOTE: L'abilitazione della policy **All Blocked / User Defined** è consigliata solo ad un'utenza esperta e con conoscenze approfondite delle comunicazioni di livello IP.

NOTE: Scegliendo l'opzione **All blocked/User Defined** è necessario aggiungere nel Firewall una regola per ogni servizio. Ogni pacchetto infatti viene bloccato.

NOTE: Il Firewall, quando abilitato, blocca automaticamente ogni pacchetto, pertanto le varie regole dovranno esclusivamente permettere il passaggio del servizio.

7.4.2 Packet Filter

Queste funzioni di filtraggio dei pacchetti IP sono in buona sostanza una serie di regole che il Router applicherà ai pacchetti IP che lo attraversano. E' utile comunque sapere che il solo filtraggio sui pacchetti non elimina i problemi legati a livello di applicazioni o altri livelli.
Le politiche con cui organizzare il filtraggio sono essenzialmente riassumibili in 2 differenti filosofie:

- **Passa solo quello che ritengo sicuro il resto è bloccato**
- **Blocco quello che ritengo pericoloso e tutto il resto passa.**

Tali politiche dovrebbe essere applicata da coloro che possiedono una buona conoscenza di Internet (in particolar modo nel primo approccio) in quanto è necessario creare una regola per ogni "servizio" che si vuole usare.
Una volta che si attiva il Firewall del Router di fatto TUTTO il traffico non espressamente permesso viene bloccato (posizione 1).

Nel caso in cui si sia selezionata una policy di firewalling predefinita, è possibile modificare le regole esistenti al fine di adattare la struttura del Firewall alle proprie esigenze specifiche.
Per modificare una regola predefinita, selezionare la regola da modificare attraverso il tasto di selezione **Edit** come indicato in figura:

Packet Filter

Parameters			
Rule Name Helper	mei_http << --Select--		
Time Schedule	Always On		
Source IP Address(es)	0.0.0.0	Netmask	0.0.0.0
Destination IP Address(es)	0.0.0.0	Netmask	0.0.0.0
Type	TCP	Protocol Number	
Source Port	0 - 65535		
Destination Port	80 - 80		
Inbound	Block		
Outbound	Allow		

Add | Edit / Delete

Edit	Rule Name	Time Schedule	Source IP / Netmask Destination IP / Netmask	Protocol	Source port(s) Destination port(s)	Inbound Outbound	Delete
◉	mei_http	Always On	0.0.0.0 / 0.0.0.0 0.0.0.0 / 0.0.0.0	TCP	0 ~ 65535 80 ~ 80	Block Allow	○
○	mei_msntcp	Always On	0.0.0.0 / 0.0.0.0 0.0.0.0 / 0.0.0.0	TCP	0 ~ 65535 1863 ~ 1863	Block Allow	○

A questo punto sarà possibile modificare ogni singola opzione della regola selezionata. Al termine della modifica, premere il tasto **Edit/Delete** per confermare le modifiche.

Per cencellare una regola predefinita, selezionare la regola da eliminare attraverso il tasto di selezione **Delete** e confermare tramite la pressione del tasto **Edit/Delete**

Vedremo ora come aggiungere una nuova regola di firewalling all'interno della lista di filtering del WebShare 3G 244WN.

Add TCP/UDP Filter

Parametro	Descrizione
Rule name	Inserire il nome identificativo della regola di firewall oppure selezionare un servizio dalla lista di regole predefinite. La lunghezza massima del campo non può superare i 32 caratteri.
Time Schedule	Permette di impostare la validità temporale della regola. Fare riferimento alla sezione **Time schedule** per ulterioi dettagli.
Source IP Address(es)	Inserire l'indirizzo o il range di indirizzi di provenienza del pacchetto e relativa nesmask.
Destination IP Address(es)	Inserire l'indirizzo o il range di indirizzi di destinazione del pacchetto e relativa nesmask.
Type	Definire la tipologia di pacchetto da filtrare (TCP, UDP o entrambi).
Protocol Number	Questa opzione non è attiva in questo tipo di configurazione.
Source Port	Inserire la porta o il range di porte sorgente da filtrare.
Destination Port	Inserire la porta o il range di porte destinazione del pacchetto

Inbound/Outbound	Selezionare se permettere (Allow) o bloccare (Block) il traffico in ingresso (Inbound) ed in uscita (Outbound).

Per bloccare un singolo indirizzo IP, nel campo **Netmask** sarà necessario impostare il valore 255.255.255.255 associandolo all'indirizzo IP da bloccare.

Premere il tasto **Add** per aggiungere la regola appena creata.

Add Raw IP Filter

Per applicare un filtraggio a livello di protocollo, procedure come segue:

Parametro	Descrizione
Rule name	Inserire il nome identificativo della regola di firewall. La lunghezza massima del campo non può superare i 32 caratteri.
Time Schedule	Permette di impostare la validità temporale della regola. Fare riferimento alla sezione **Time schedule** per ulterioi dettagli.

Source IP Address(es)	Inserire l'indirizzo o il range di indirizzi di provenienza del pacchetto e relativa nesmask.
Destination IP Address(es)	Inserire l'indirizzo o il range di indirizzi di destinazione del pacchetto e relativa nesmask.
Type	Selezionare l'opzione **Use Protocol Number**.
Protocol Number	Inserirei il numero di protocollo da filtrare.
Source Port	Questa opzione non è attiva in questo tipo di configurazione.
Destination Port	Questa opzione non è attiva in questo tipo di configurazione.
Inbound/Outbound	Selezionare se permettere (Allow) o bloccare (Block) il traffico in ingresso (Inbound) ed in uscita (Outbound).

Premere il tasto **Add** per aggiungere la regola appena creata.

7.4.3 Intrusion Detection

Il Router può automaticamente riconoscere e bloccare un attacco di tipo DoS (Denial of Service) o Port Scan se la funzione di Intrusion Detection è attiva. Lo scopo di attacchi appartenenti a questa tipologia non è quello di cogliere informazioni particolari dalla LAN quanto piuttosto renderla inutilizzabile per un certo periodo di tempo. Il Firewall inoltre supporta la funzionalità Blacklist per minimizzare l'efficacia degli attacchi. La Blacklist è vuota nel momento dell'attivazione del Firewall. Quando il Router si accorge di essere stato attaccato memorizza nella blacklist l'IP da cui proviene l'attacco. L'IP di ogni pacchetto ricevuto dal Router, prima di essere processato, viene confrontato con quelli presenti nella blacklist (e se presente viene scartato). A seconda del tipo di attacco, l'IP verrà mantenuto « inattivo » per un determinato periodo di tempo (scaduto il quale verrà cancellato dalla Blacklist).

Questo modulo del Firewall è attivabile solo se in General Settings è stato impostato uno dei 4 livelli di sicurezza previsti.

Vediamo nel dettaglio le tipologie di attacchi DoS:

- **Attacchi che mirano all'esaurimento della banda**, sono realizzabili in due modalità diverse a seconda di quanta banda abbia l'attaccante.

Qualora la banda sia maggiore dell'attaccato può saturarlo diversamente può usare altri host che di fatto amplificano l'attacco.

- **Attacchi che mirano all'esaurimento delle risorse**.
- **Attacchi contro difetti di programmazione**, che mirano a sfruttare bug software o hardware.
- **Attacchi DoS generici**.

Vediamo come attivare e configurare la funzionalità di **Intrusion Detection** integrata all'interno del Firewall del WebShare 3G 244WN:

Parametro	Descrizione
Intrusion Detection	Abilita la funzionalità di rilevamento delle intrusioni e la relativa blacklist. La blacklist è un registro nel quale vengono aggiunti di volta in volta gli indirizzi IP ritenuti responsabili degli attacchi in oggetto. Dal momento di inserimento all'interno della BlackList, ogni tentativo di comunicazione da parte dell'IP in questione sarà inibito per un intervallo definito dai campi Block Duration, relativamente ad ogni tipologia di attacco. La pulizia della blacklist sarà possibile attraverso la pressione

	del tasto **Clear Blacklist**.
Victim Protection Block Duration	Determinato un attacco di tipo Smurf, il router blocca il traffico dall'host esterno (il cui IP è stato inserito nella blacklist) per un intervallo di tempo stabilito.
Scan Attach Block Duration	Determinato un attacco di tipo Scan, il router blocca il traffico dall'host esterno (il cui IP èstato inserito nella blacklist) per un intervallo di tempo stabilito. Tipici attacchi Scan sono **X'mas scan**, **IMAP Syn/Fin scan**.
DOS Attack Block Duration	Dopo che un attacco di tipo DoS è stato rilevato, il router blocca il traffico dall'host esterno (il cui IP è stato inserito nella blacklist) per un intervallo di tempo stabilito. Tipici attacchi DoS sono **WinNuke** ed **Ascend Kill**.
Maximum TCP Open Handshaking Count	Stabilisce il massimo numero di sessioni TCP aperte (in fase di handshaking) per secondo. Qualora questo numero venga raggiunto il router considera questo come un attacco **SYN Flood**.
Maximum Ping Count	Stabilisce il massimo numero pacchetti tipo PING per secondo. Qualora questo numero venga raggiunto il router considera questo come un attacco **ECHO Storm**.
Maximum ICMP Count	Stabilisce il massimo numero pacchetti tipo ICMP per secondo. Qualora questo numero venga raggiunto (sono esclusi Echo Request) il router considera questo come un attacco **ICMP Flood.**

Premere **Apply** per applicare le modifiche.

Riguardo ad attacchi di tipo SYN Flood, ICMP Echo Storm e ICMP flood, il modulo IDS si limiterà ad inserire nell'Event Log la segnalazione opportuna. Non viene attuata alcuna protezione contro tali attacchi.

Di seguito si riporta una serie di attacchi che il modulo IDS integrato è in grado di riconoscere ed una breve descrizione degli attacchi più comuni:

Intrusion Name	Detect Parameter	Blacklist	Type of Block Duration	Drop Packet	Show Log
Ascend Kill	Ascend Kill data	Src IP	DoS	Yes	Yes
WinNuke	TCP Port 135, 137~139, Flag: URG	Src IP	DoS	Yes	Yes
Smurf	ICMP type 8 Des IP is broadcast	Dst IP	Victim Protection	Yes	Yes
Land attack	SrcIP = DstIP			Yes	Yes
Echo/CharGen Scan	UDP Echo Port and CharGen Port			Yes	Yes
Echo Scan	UDP Dst Port = Echo(7)	Src IP	Scan	Yes	Yes
CharGen Scan	UDP Dst Port = CharGen(19)	Src IP	Scan	Yes	Yes

X'mas Tree Scan	TCP Flag: X'mas	Src IP	Scan	Yes	Yes
IMAP SYN/FIN Scan	TCP Flag: SYN/FIN DstPort: IMAP(143) SrcPort: 0 or 65535	Src IP	Scan	Yes	Yes
SYN/FIN/RST/ACK Scan	TCP, No Existing session And Scan Hosts more than five.	Src IP	Scan	Yes	Yes
Net Bus Scan	TCP No Existing session DstPort = Net Bus 12345,12346, 3456	SrcIP	Scan	Yes	Yes
Back Orifice Scan	UDP, DstPort = Orifice Port (31337)	SrcIP	Scan	Yes	Yes
SYN Flood	Max TCP Open Handshaking Count (Default 100 c/sec)				Yes
ICMP Flood	Max ICMP Count (Default 100 c/sec)				Yes
ICMP Echo	Max PING Count				Yes

	(Default 15 c/sec)				

Src IP: Source IP**, Src Port:** Source Port**, Dst Port:** Destination Port**, Dst IP:** Destination IP

Segue una breve descrizione del funzionamento degli attacchi più comuni:

- **IP Spoofing:** è un attacco particolare in cui l'attaccante cerca di intromettersi in una connessione con lo scopo di abbatterla o di prenderne il controllo. Può essere fatto sia dall'interno della propria Lan (con possibilità più alte di successo se si dispone di LAN con HUB) che da Internet con possibilità di successo infinitamente inferiori. Grazie all' SPI il Router esamina a fondo i pacchetti che lo attraversano e confrontando molti parametri coi pacchetti precedenti della stessa connessione riesce a stabilire con efficacia se un pacchetto in arrivo è "spoofato" o meno.
- **Sync Flood**: come già accennato è un attacco che mira a esaurire le risorse del sistema che lo subisce. All'atto dell'instaurazione di una connessione viene spedito un pacchetto (dall'attaccante) col quale si avvisa che si vuole costruire la connessione. Il ricevente, cioè l'attaccato, alloca delle risorse e risponde con un pacchetto per proseguire la creazione della connessione. L'attaccato aspetta pazientemente il pacchetto di risposta (che non arriverà mai poiché l'attaccante avrà scelto o un IP di un host spento oppure starà attaccando l'host in questione impedendogli di rispondere). Le risorse allocate saranno bloccate sino a che non scade il timer associato. Nel frattempo l'attaccante ripeterà quest'attacco finendo col bloccare tutte le risorse disponibili nell'attaccato. Il firewall integrato nell' ADSL Router riconosce il tentativo di apertura di diverse connessioni provenienti dallo stesso IP e non allocherà le risorse. Certamente, a meno di trovarsi con sprovveduti, l'IP che verrà registrato nella tabella del sicurity logs non apparterrà all'attaccante.
- **Smurf Attack**: tenta invece di esaurire l'intera banda dell'host vittima, per fare questo può (a seconda della velocità della sua connessione) sfruttare anche delle sottoreti che fungono da amplificatore. Infatti l'indirizzo di broadcast di queste sottoreti vieni sfruttato e così tutti gli host di questa sottorete rispondono all'Echo Request richiesto dall'attaccante che avrà sostituito l'IP del mittente con quello dell'attaccato. All'attaccato tutti gli host risponderanno col pacchetto di Echo Reply generando un traffico

intensissimo. Il Router filtra i pacchetti di Echo Reply in uscita trattandolo come un attacco.

- **Ping of Death:** quest'attacco particolare e dalle conseguenze variabili (anche a seconda del carico della macchina) viene generato creando un pacchetto ICMP di Echo Request fuori standard. Il pacchetto IP può infatti essere lungo, dalle spefiche RFC, al massimo 65536 bytes di cui 20 sono riservati per l'header. Entro il Payload vengono inseriti i pacchetti di livello superiore, in questo caso l'ICMP (oppure TCP, UDP) che ha un header lungo 8 bytes. La lunghezza massima per il Payload del pacchetto ICMP è dunque 65535-20-8=60507 bytes. Sebbene un pacchetto del genere sia fuori specifica è comunque realizzabile, inoltre arriva frammentato alla destinazione (l'attaccato) dove verrà ricomposto (non verificandolo prima) ma a questo punto potrebbe generare un overflow dello stato di alcune variabili. Il firewall integrato si accorge di questo tipo di attacco e scarta il pacchetto in questione, aggiornando la tabella del security logs.
- **Land Attack:** sfrutta un errore presente in molti Sistemi operativi o Router che quando ricevono un particolare pacchetto (il cui IP di provenienza è uguale a quello di destinazione, cioè l'attaccato) di richiesta di connessione tentano di stabilirla ma vanno incontro ai più diversi blocchi. In pratica l'attaccato cerca di colloquiare con se stesso. Il Router elimina tutti i pacchetti con questa caratteristica.

7.4.4 URL Filter

Tramite questa funzionalità è possibile filtrare ulteriormente il traffico in uscita limitando tale traffico in base all'ora e/o giorno, al tipo di URL e ad una parola contenuta all'interno dell'URL stessa. E' possibile altresì attivare il blocco di alcuni elementi potenzialmente dannosi per il sistema comunemente utilizzati per la propagazione delle infezioni (quali ad esempio le applet Java).
Grazie all'approfondita gestione delle politiche di filtraggio, e' possibile bloccare l'accesso ad alcuni siti oppure consentire l'accesso solo ad una lista opportuna. E' inoltre possibile impedire l'accesso ad alcuni URL che hanno una determinata sequenza di caratteri.

Per attivare questa funzionalità anzitutto spuntare la voce **Enable** (come da figura).

Parametro	Descrizione
URL Filtering	Abilita la funzionalità di filtraggio URL.
Block Mode	Indica la validità temporale di questa tipologia di filtro (Fare riferimento alla sezione **Time Schedule** per approfondimenti). Selezionare l'opzione **Disabled** per disattivare questa tipologia di filtraggio.
Keywords Filtering	Questa funzionalità permette di attivare un filtro URL sulla base delle parole contenute all'interno dell'host name interrogato (fare riferimento al paragrafo dedicato per approfondimenti).

Domains Filtering	Questa funzionalità permette di attivare un filtro URL dei domini indicati. Selezionando l'opzione **Disable all WEB traffic except for Trusted Domains** per bloccare tutto il traffic tranne quello verso i domini autorizzati (fare riferimento al paragrafo dedicato per approfondimenti).
Restricted URL Features	Permette di filtrare le applet Java presenti in molti siti web e di inibire la navigazione tramite indirizzo IP (bypassando cosi il blocco sui nomi di dominio).
Exception List	E' possibile indicare una lista di indirizzi IP che non verranno sottoposti alle policy di filtraggio URL configurate.

Keywords Filtering

La funzionalità Keyword Filtering permette di inibile l'accesso a tutti i siti che contengano, all'interno della propria URL, una o più parole specificate nella lista di bloccaggio.
Per comprendere al meglio questa funzionalità, si pensi di voler bloccare tutti i domini contenenti la parola SEX:

1. Abilitare la funzionalità **Keyword Filtering** dal menu principale e premere su **Details** per effettuare la configurazione dei criteri di filtraggio.

2. Inserire la parola che si desidera bloccare nel campo Keyword e premere il tasto **Add.**

3. Mano a mano che verranno inserite le parole da bloccare, la lista **Block WEB URLSs which contains these keywords** comincerà a popolarsi, associando un nome generico progressivo ad ogni singola entry (itemX).

4. Per cancellare la regola, selezionare la stessa come da figura e confermare la selezione premendo il tasto **Delete**.

Una volta terminato l'inserimento, premere su **Return** per tornare alla schermata principale della sezione.

Domains Filtering

Grazie a questa funzionalità, è possibile permettere l'accesso da parte dei client esclusivamente ad una lista di domini determinata.
Le politiche con cui organizzare il filtraggio sono essenzialmente riassumibili in 2 differenti filosofie:

- **Blocco i domini indicati e permetto l'accesso a tutto ciò che non è esplicitamente dichiarato.**
- **Consento l'accesso esclusivamente ai domini dichiarati e blocco tutto il resto.**

Nello specifico, di seguito verranno indicate entrambe le filosofie di filtering, cosi da poter fornire un'ampia gamma di soluzioni anche all'utilizzatore più esperto.

Di seguito è riportata la procedura per la configurazione in relazione alla prima politica di filtraggio ndicata:

1. Abilitare la funzionalità **Domains Filtering** dal menu principale e premere su **Details** per effettuare la configurazione dei criteri di filtraggio.

2. Inserire il dominio sul quale si intende applicare la politica di filtraggio ed impostare la modalità Type in **Forbidden Domain**. Premere sul pulsante **Add** per aggiungere il dominio alla lista dei domini bloccati.

In questo modo, il WebShare 3G 244WN inibirà la navigazione verso i tutti quei domini dichiarati come **Forbidden Domain**.
Di seguito è invece riportata la procedura per la configurazione in relazione alla seconda politica di filtraggio indicata:

1. Abilitare le funzionalità **Domains Filtering** e **Disable all WEB Traffic except for Trusted Domains** dal menu principale e premere su **Details** per effettuare la configurazione dei criteri di filtraggio.

2. Inserire il dominio sul quale si intende applicare la politica di filtraggio ed impostare la modalità Type in **Truster Domain**. Premere sul pulsante **Add** per aggiungere il dominio alla lista dei domini consentiti.

In questo modo, il WebShare 3G 244WN inibirà la navigazione verso i tutti i domini Internet, ad eccezione di quelli dichiarati come **Trusted Domain**.
Per l'eliminazione di un dominio dalla lista Forbidden o Trusted, selezionare il dominio tramite il tasto di selezione e premere il pulsante **Delete** per confermare l'operazione.

7.4.5 IM/P2P Blocking

Grazie a questa funzionalità, è possibile filtrare i più comuni software di Instant Messaging ed i client di condivisione file quali BitTorrent e/o eDonkey.

Parametro	Descrizione
Instant Message Blocking	Abilita la funzionalità di filtering per i più comuni programmi di Instant Messaging sotto riportati.
Yahoo Messenger	Spuntare questa opzione se si desidera bloccare il programma indicato.
MSN Messeger	Spuntare questa opzione se si desidera bloccare il programma indicato.
Peer to Peer Blocking	Abilita la funzionalità di filtering per i più comuni programmi di P2P sotto riportati.
BitTorrent	Spuntare questa opzione se si desidera bloccare il programma indicato.
eDonkey	Spuntare questa opzione se si desidera bloccare il programma indicato.

Premere sul pulsante **Apply** per confermare.

Anche per questa funzionalità. Sarà possibile schedulare intervalli di funzionamento predefiniti. Fare riferimento al capitolo **Time Schedule** per ulteriori approfondimenti.

Il continuo rilascio di nuove versioni dei programmi/client indicati può rendere inefficace questa tipologia di filtro. Si consiglia di verificare la disponibilità di aggiornamenti firmware sul sito www.atlantis-land.com al fine di mantenere aggiornate le funzionalità del prodotto.

7.4.6 Firewall Log

Tramite questa sezione sarà possibile selezionare quali tipologie di minaccie verranno inserite all'interno del visualizzatore di eventi dell'apparato (Event Log). Impostare il campo su Enable per registrare gli eventi di questa tipologia all'interno del registro di sistema.

7.5 Qos (Quality of Service)

Il dispositivo per eccellenza nella LAN in cui si attua la multiplazione statistica delle risorse è indubbiamente l'apparato responsabile della connettività, nel caso in esame l'Adsl2+ Router. In effetti il Router ADSL permette, indipendentemente dalla tipologia di contratto fornita dall'ISP, ad una moltitudine di PC di condividere la singola connessione ADSL. Generalmente questa situazione rappresenta spesso un collo di bottiglia, in quanto ciascun PC vorrebbe poter utilizzare il massimo della connettività offerta dal Router che invece deve permettere, sempre e comunque, agli altri utenti di accedere alla risorsa.
In una LAN tradizionale non esiste un altro dispositivo responsabile della gestione di una così marcata multiplazione. L'accesso dati verso un server centralizzato, nel caso di rete correttamente strutturata con dorsale in gigabit, non rappresenta solitamente un problema visto il corretto dimensionamento delle risorse (10 accessi

contemporanei a piena banda in F/E non sarebbero sufficienti a saturare questo collegamento).
Nel caso del Router ADSL purtroppo il limite è fornito dalla velocità della connessione ADSL spesso limitata ad una frazione di megabit. In questo megabit, dozzine di utenti, devono poter effettuare Navigazione WEB, Accesso/Invio della propria posta, effettuare download, servizi di streaming e così via.
Il risultato complessivo genera solitamente un accumulo di richieste inviate verso il Router e da questo bufferizzate in attesa di essere processate non appena le risorse siano nuovamente disponibili. La logica utilizzata dal Router è solitamente di tipo FIFO. In questo scenario, tipico già nella piccola azienda, abbiamo un'enorme crescita dei tempi di latenza che generano:

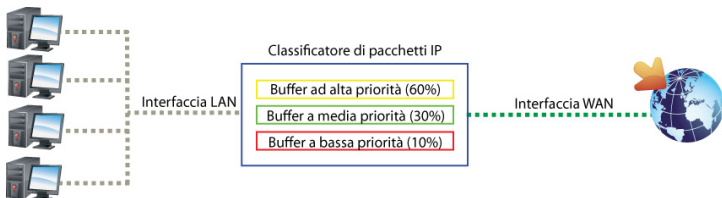
- Attesa via via crescenti
- Impossibilità nell'uso di servizi in tempo reale (VoIP, Streaming, Netmeeting)
- Scadere di taluni Timeout
- Lo scadere di un Timeout genera la ritrasmissione di interi pacchetti, ciò produce un enorme spreco di risorse avvicinando così la rete verso la congestione.

Il Router ADSL permette di risolvere/limitare questo problema cambiando radicalmente la politica utilizzata nel processare i pacchetti IP inviatigli. Ogni pacchetto ricevuto dal Router viene anzitutto classificato, in base a criteri specificati dall'amministratore, e quindi memorizzato, laddove non ci siano le risorse disponibili, in un buffer opportuno. Il dispositivo permette per ogni servizio/applicazione:

- di garantire una percentuale minima di banda
- limitare un massimo di banda

questo tanto in upload che download.
Il Router dunque non processa più con logiga FIFO il buffer dei pacchetti ma prima classifica il pacchetto, in base alle policy, e poi assegna le risorse disponibili.
I vantaggi derivanti dall'uso di attente politiche di Priorità sono:

- Attesa media contenuta
- Riduzione di overhead di ritrasmissione
- Piena fruibilità di servizi quali VoIP, Netmeeting, Streamin e così via.

Questo da una parte genera un più razionale utilizzo della risorsa comune e rende meno probabili le condizioni che portano alla saturazione della rete.
Nella figura sottostante è possibile vedere il diagramma a blocchi del dispositivo.

Resta inteso che dare ad ogni servizio/IP priorità massima, significa di fatto accorpare gran parte del traffico in un solo buffer che viene comunque processato con logica FIFO. Questo non porta a nessun risultato apprezzabile.

7.5.1 Prioritization

All'interno del WebShare 3G 244WN, sono disponibili 3 differenti livelli di priorità:

- **High:** il dispositivo alloca a questa tipologia di traffico il 60% della banda disponibile.
- **Normal:** il dispositivo alloca a questa tipologia di traffico il 30% della banda disponibile.
- **Low:** il dispositivo alloca a questa tipologia di traffico il 10% della banda disponibile.

Tutto il traffico non specificatamente assegnato ai buffer High/Low verrà classificato come Normal

Per creare una nuova regola di prioritizzazione del traffico, si prega di seguire la procedura sottoindicata:

Prioritization

Configuration (from LAN to WAN packet)			
Name		Time Schedule	Always On
Priority	High	Protocol	any
Source IP Address Range	0.0.0.0 ~ 0.0.0.0	Source Port	0 ~ 0
Destination IP Address Range	0.0.0.0 ~ 0.0.0.0	Destination Port	0 ~ 0
DSCP Marking	Disabled		

Add | Edit / Delete

Edit	Name	Time Schedule	Protocol	Priority	DSCP Marking	Delete

Parametro	Descrizione
Name	Inserire il nome da associare alla regola.
Time Schedule	Selezionare **Always-On** per mantenere la regola sempre attiva oppure uno dei 16 time slot configurabili. Per ulteriori dettagli fare riferimento al paragrafo dedicato.
Priority	Impostare il livello di priorità da assegnare al traffico in grado di soddisfare questa regola. Si ricorda che: • **High:** alloca il 60% della banda istantanea disponibile • **Normal:** alloca il 30% della banda istantanea disponibile • **Low:** alloca il 10% della banda istantanea disponibile
Source IP Address Range	Inserire l'indirizzo o il range di indirizzi IP sorgente che verranno sottoposti alla monitorizzazione.

Source Port	Inserire la porta servizio o il range di porte sorgente che verranno sottoposte alla monitorizzazione.
Destination IP Address Range	Inserire l'indirizzo o il range di indirizzi IP destinazione che verranno sottoposti alla monitorizzazione.
Destination Port	Inserire la porta servizio o il range di porte destinazione che verranno sottoposte alla monitorizzazione.
DSCP Marking	Permette di marcare il traffico soddisfacente questa regola secondo le specifiche DSCP, al fine di propagare la QoS anche su reti IP (se supportato dai Gateway).

Per poter usufruire della QoS su Protocollo DSCP, è necessario che i gateway della rete Internet siano in grado di interpretare correttamente il campo DSCP contenuto nel pacchetto IP.

Premere il pulsante **Add** per aggiungere la regola appena creata alla lista.

Per cancellare una regola preesistente, selezionarla tramite il pulsante di selezione **Delete** e confermare l'operazione premendo il bottone **Edit/Delete**.

Per modificare una regola preesistente, selezionare la regola tramite il pulsante **Edit** ed eseguire le modifiche del caso.

Al termine delle modifiche, premere il pulsante **Edit/Delete** per confermare le modifiche.

Di seguito viene riportata una tabella associativa dei livelli di marcatura del prodotto relativamente agli stati proposti dallo standard DSCP:

DSCP Mapping Table

WebShare 3G 244WN	Standard DSCP
Disabled	None
Best Effort	Best Effort (000000)
Premium	Express Forwarding (101110)
Gold service (L)	Class 1, Gold (001010)
Gold service (M)	Class 1, Silver (001100)

Gold service (H)	Class 1, Bronze (001110)
Silver service (L)	Class 2, Gold (010010)
Silver service (M)	Class 2, Silver (010100)
Silver service (H)	Class 2, Bronze (010110)
Bronze service (L)	Class 3, Gold (011010)
Bronze service (M)	Class 3, Silver (011100)
Bronze service (H)	Class 3, Bronze (011110)

7.5.2 IP Throttling (Outbound e Inbound)

La funzionalità IP Throttling (disponibile sia per il traffico LAN to WAN che WAN to LAN), permette di limitare in maniera static la banda dedicate a determinati servizi/indirizzi IP (in multipli di 32kbps). Questo fa si che sia permessa la limitazione del traffico IP di una ben determinata workstation oppure che il traffico generato dal server FTP presente in rete non superi mai un limite di velocità ben definito.

Parametro	Descrizione
Name	Inserire il nome da associare alla regola.
Time Schedule	Selezionare **Always-On** per mantenere la regola sempre attiva oppure uno dei 16 time slot configurabili. Per ulteriori dettagli fare riferimento al paragrafo dedicato.
Protocol	Impostare il protocollo sul quale attivare la regola (selezionando l'opzione **Any**, la regola verrà attivata su qualsiasi protocollo)
Rate Limit	Impostare il limte di velocità (in multipli di 32kbps) che si intende imporre al traffico in grado di soddisfare i requisiti della regola.
Source IP Address Range	Inserire l'indirizzo o il range di indirizzi IP sorgente che verranno sottoposti alla monitorizzazione.
Source Port	Inserire la porta servizio o il range di porte sorgente che

	verranno sottoposte alla monitorizzazione.
Destination IP Address Range	Inserire l'indirizzo o il range di indirizzi IP destinazione che verranno sottoposti alla monitorizzazione.
Destination Port	Inserire la porta servizio o il range di porte destinazione che verranno sottoposte alla monitorizzazione.
DSCP Marking	Permette di marcare il traffico soddisfacente questa regola secondo le specifiche DSCP, al fine di propagare la QoS anche su reti IP (se supportato dai Gateway).

Premere il pulsante **Add** per aggiungere la regola appena creata alla lista.

Per cancellare una regola preesistente, selezionarla tramite il pulsante di selezione **Delete** e confermare l'operazione premendo il bottone **Edit/Delete**.

Per modificare una regola preesistente, selezionare la regola tramite il pulsante **Edit** ed eseguire le modifiche del caso.

Al termine delle modifiche, premere il pulsante **Edit/Delete** per confermare le modifiche.

7.6 Virtual Server

Il NAT dell' Adsl2+ VPN Router consente la protezione della LAN locale da parte di accessi esterni indesiderati. Può essere necessario comunque consentire ad utenti esterni l'accesso ad un PC specifico della Lan (per esempio verso un PC che offre funzionalità di server Web o FTP). La funzionalità di Virtual Server consente di reindirizzare un particolare servizio, che avviene su una determinata porta, su un PC della Lan interna. E' possibile scegliere la porta ed il protocollo che si intende rigirare sull'indirizzo IP privato.

7.6.1 Port Forwarding

Questa funzionalità permette di impostare il Router in modo che un determinate tipo di traffico in arrive sull'interfaccia sterna (WAN) possa essere correttamente reindirizzato ad uno specifico indirizzo IP della rete LAN.
Molte delle applicazioni diffuse oggi in Internet (FTP Server, Web Hosting, etc), necessitano di una configurazione della sezione Port Forwarding in modo che le richieste provenienti da client esterni vengano correttamente inoltrare ai rispettivi server che si occuperanno di fornire una risposta a queste ultime.
Di seguito si riporta la procedura per la creazione di una nuova regola di port forwarding:

Parametro	Descrizione
Via WAN Interface	Definire l'interfaccia esterna (WAN) per la quale sarà valida la regola.
Application	Inserire un nome per la regola oppure selezionare una regola predefinita dalla lista a scomparsa.
Protocol	Selezionare il protocollo da monitorare.
Time Schedule	Selezionare l'opzione **Always On** per attivare in maniera permanente la regola oppure uno dei 16 profili predefiniti. Per informazioni avanzate, fare riferimento al paragrafo relativo.
External Port	Impostare la porta servizio sulla quale il Router dovrà rimanere in attesa del pacchetto da reindirizzare.
Redirect Port	Impostare la porta servizio verso la quale dovrà essere reindirizzato il pacchetto entrante che soddisfi la regola.
Internal IP Address	Inserire l'indirizzo IP di un PC presente in LAN verso il quale indirizzare tutti i pacchetti che soddisfino la regola. E' possibile selezionare un indirizzo IP anche dal menu a tendina.

Premere il pulsante **Add** per aggiungere la regola appena creata alla lista.

Per cancellare una regola preesistente, selezionarla tramite il pulsante di selezione **Delete** e confermare l'operazione premendo il bottone **Edit/Delete**.

Per modificare una regola preesistente, selezionare la regola tramite il pulsante **Edit** ed eseguire le modifiche del caso.

Al termine delle modifiche, premere il pulsante **Edit/Delete** per confermare le modifiche.

NOTE: Qualora l'opzione di NAT sia disabilitata la funzionalità di Virtual Server non è utilizzabile.

NOTE: Se sul Router è abilitato il DHCP bisogna prestare particolare attenzione ad assegnare l'indirizzo IP dei Virtual Server per evitare conflitti. In questo caso è sufficiente assegnare al PC Server (Tale PC non sarà client DHCP ed avrà oltre all'indirizzo IP, la subnet mask, il gateway (cioè l'IP privato del Router ADSL) ed i server DNS) un indirizzo IP che sia nella stessa subnet dell' Adsl2+ VPN Router ma fuori dal range di indirizzi IP assegnabili dal server DHCP attivo sul Router.

NOTE: Il Router può gestire un numero non infinito di connessioni entranti, pertanto per grandi range potrebbero sorgere problemi ed il servizio di VS funzionare in maniera impropria.

NOTE: Se l'applicazione non è inclusa nella lista di sopra, consultare il sito web del produttore dell'applicazione per conoscere le porte da ruotare. L'assistenza tecnica non fornirà dettagli sulle porte utilizzate dai vari

software e/o applicativi che sono di esclusiva pertinenza della softwarehouse che ha sviluppato l'applicazione. Si invita pertanto a contattare tale softwarehouse.

Alcune applicazioni Internet ormai oggi diffusissime necessitano, per essere usate pienamente, di una configurazione particolare della sezione Virtual Server del WebShare Router. Nella lista seguente sono presenti questi settaggi. La lista non vuole essere esaustiva ma solo un punto d'inizio, invitiamo a consultare eventuali aggiornamenti di questo manuale (scaricabile dal sito www.atlantis-land.com).

Applicazione	Connessioni Uscenti	Connessioni Entranti
ICQ 98, 99a	Nessuno	Nessuno
NetMeeting 2.1 a 3.01	Nessuno	1503 TCP, 1720 TCP
VDO Live	Nessuno	Nessuno
mIRC	Nessuno	Nessuno
Cu-SeeMe	7648 TCP &UDP, 24032 UDP	7648 TCP &UDP, 24032 UDP
PC AnyWhere	5632 UDP, 22 UDP, 5631 TCP, 65301 TCP	5632 UDP, 22 UDP, 5631 TCP, 65301 TCP
Edonkey/Emule	Nessuno	principalmente 4660-4662 TCP , 4665-4672 UDP
MSN Messanger	Nessuno	TCP da 6891-6900 TCP 1863 TCP 6901 UDP 1863 UDP 6901 UDP 5190
VNC	Nessuno	TCP 5900

Il Router può gestire un numero non infinito di connessioni, pertanto per grandi range (o centinaia di connessioni cintemporanee) potrebbero sorgere problemi.
Questo dispositivo supporta sino a 1500 connessioni contemporanee, quindi regolare i vari software di P2P affinché tale valore sia rispettato (in caso di dubbi chiamare l'assistenza tecnica).

Di seguito una serie di porte notevoli:

Servizio	Numero di Porta / Protocollo
File Transfer Protocol (FTP) Data	20/tcp
FTP Commands	21/tcp
Telnet	23/tcp
Simple Mail Transfer Protocol (SMTP) Email	25/tcp
Domain Name Server (DNS)	53/tcp and 53/udp
Trivial File Transfer Protocol (TFTP)	69/udp
finger	79/tcp
World Wide Web (HTTP)	80/tcp
POP3 Email	110/tcp
SUN Remote Procedure Call (RPC)	111/udp
Network News Transfer Protocol (NNTP)	119/tcp
Network Time Protocol (NTP)	123/tcp and 123/udp
News	144/tcp
Simple Management Network Protocol (SNMP)	161/udp
SNMP (traps)	162/udp
Border Gateway Protocol (BGP)	179/tcp
Secure HTTP (HTTPS)	443/tcp
rlogin	513/tcp
rexec	514/tcp
talk	517/tcp and 517/udp
ntalk	518/tcp and 518/udp
Open Windows	2000/tcp and 2000/udp
Network File System (NFS)	2049/tcp
X11	6000/tcp and 6000/udp
Routing Information Protocol (RIP)	520/udp
Layer 2 Tunnelling Protocol (L2TP)	1701/udp

Al fine di garantire una migliore comprensione di quanto trattato, di seguito un esempio di configurazione.

Si ponga di avere un server WEB attivo sulla propria rete LAN, ospitato su una macchina con indirizzamento IP 192.168.1.100; questo server deve essere in grado di rispondere alle richieste provenienti dai client esterni.
Posto che il gateway verso Internet per la macchina ospite del server WEB sia il WebShare 3G 244WN, sarà necessario creare una regola di port forwarding come segue:

In questo caso, è stato possibile avvalersi di una delle regole reimpostate per reindirizzare il traffico HTTP verso il server 192.168.3.1

7.6.2 Edit DMZ Host

Un PC sottoposto a DMZ è a tutti gli effetti un computer esposto ad Internet; in questa configurazione, un pacchetto in ingresso viene esaminato dal Firewall (passa il NAT) e passato all'indirizzo contenuto nel DMZ (se non soddisfa un Virtual Server).
Sarà possibile impostare un solo indirizzo IP come DMZ Host in quanto tutto il traffico che non sia in grado di soddisfare una regola di Port Forwarding verrà indirizzato verso questo client.
Per la configurazione, è necessario solamente spuntare il campo **Enabled** ed inserire nel campo **Internal IP Address** l'indirizzamento dell'host DMZ (Sarà possibile selezionarlo altresì dalla lista a scomparsa).

Parametro	Descrizione
Via WAN Interface	Definire l'interfaccia esterna (WAN) per la quale sarà valida la regola.
Enabled/Disabled	Attiva o disattiva la funzionalità DMZ Host.
Internal IP Address	Inserire l'indirizzo IP di un PC presente in LAN verso il quale indirizzare tutti i pacchetti che non soddisfino alcuna regola di port forwarding. E' possibile selezionare un indirizzo IP anche dal menu a tendina.

Premere il pulsante **Apply** per confermare le modifiche.

Se abilitata, la funzionalità DMZ consente la rotazione di tutti i protocolli verso un determinato indirizzo IP privato della Lan. Può essere abilitata per consentire il passaggio di determinati servizi. Resta inteso che una DMZ è una falla per la sicurezza, va pertanto utilizzata per reali necessità.

7.6.3 Edit One-to-One NAT (Network Address Translation)

La funzionalità One-to-One NAT mappa specifici indirizzi IP locali su IP pubblici detti anche Global IP. Se si hanno a disposizione più IP pubblici, assegnati dal provider, è possibile utilizzarli come descritto in questa sezione.

Global IP Pool

Global Address Pool					
via WAN Interface	ipwan				
NAT Type	◉ Disable ○ Public to Private Subnet ○ Public to DMZ Zone				
Global IP Addresses	◉ Subnet	IP Address		Netmask	
	○ IP Range	IP Address		End IP	

Apply | One-to-one NAT Table

Parametro	Descrizione
Via WAN Interface	Definire l'interfaccia esterna (WAN) per la quale sarà valida la regola.
NAT Type	Selezionare la modalità di NAT che si intende utilizzare. E' possibile una tra le seguenti modalità di NAT: • **Disable:** Selezionare questa opzione nel caso in cui si disponga di un solo indirizzo IP (statico o dinamico) da condividere per la connessione ad Internet. • **Public to Private Subnet:** Consente di mappare un pool di IP pubblici su altrettanti IP privati. • **Public to DMZ Zone:** Consente di mappare un pool di IP pubblici sugli IP che fanno capo a un interfaccia DMZ. Fare riferimento alla sezione Ethernet, IP Alias per la creazione dell'interfaccia DMZ.
Global IP Address	Questa sezione permette l'immissione del pool di indirizzi IP forniti dall'ISP. Sono disponibili le seguenti modalità: • **Subnet:** Inserire indirizzo e maschera di rete del pool di IP pubblici assegnati dal provider. • **IP Range:** Inserire il primo e l'ultimo IP del pool assegnato dal provider.

Premere il pulsante **Apply** per applicare le modifiche apportate.

Premere sul pulsante One-to-one NAT Table per associare gli indirizzi precedentemente dichiarati agli IP della classe privata o DMZ:

Parametro	Descrizione
Via WAN Interface	Definire l'interfaccia esterna (WAN) per la quale sarà valida la regola.
Application	Inserire un nome per la regola oppure selezionare una regola predefinita dalla lista a scomparsa.
Protocol	Selezionare il protocollo da monitorare.
Time Schedule	Selezionare l'opzione **Always On** per attivare in maniera permanente la regola oppure uno dei 16 profili predefiniti. Per informazioni avanzate, fare riferimento al paragrafo relativo.
Global IP	Inserire l'indirizzo IP (appartenente al pool precedentemente inserito) che si intende associare ad un indirizzo privato locale o DMZ.
External Port	Impostare la porta servizio sulla quale il Router dovrà rimanere in attesa del pacchetto da reindirizzare.
Redirect Port	Impostare la porta servizio verso la quale dovrà essere reindirizzato il pacchetto entrante che soddisfi la regola.
Internal IP Address	Inserire l'indirizzo IP di un PC presente in LAN verso il quale

	indirizzare tutti i pacchetti che soddisfino la regola. E' possibile selezionare un indirizzo IP anche dal menu a tendina.

7.7 Wake On LAN

Questa funzionalità permette di "risvegliare" un PC collegato via cavo al Router mediante la generazione di un apposito pacchetto (detto pacchetto di WakeUp) instradato a livello MAC dal Router alla scheda di rete del PC da risvegliare.
Per comprendere al meglio questa funzionalità, ci serviremo di un esempio.
Si ponga di dover svegliare il PC con indirizzo MAC 00:80:AB:12:23:34; sarà necessario creare una regola di WakeOnLan come segue:

Premere il tasto **Add** per aggiungere il MAC Address contenuto nel campo relativo alla lista dei MAC Address da risvegliare.

A questo punto, basterà premere il tasto **WakeUp** per avviare la generazione del pacchetto necessario per il risveglio della macchina.

Edit	Action	MAC Address	Ready	Delete
○	Wake Up	00:80:AB:12:23:34	Yes	○

7.8 Time Schedule

La funzionalità Time Schedule consente di impostare fino a 16 TimeSlot che aiuteranno l'utente a gestire nel miglior modo la connessione ADSL. E' possibile impostare i giorni e gli orari in cui le diverse regole di firewalling, virtual server e associazioni NAT One-To-One sono attive. Questa funzionalità è strettamente correlata alla sincronizzazione dell'orologio di sistema configurabile all'interfaccia **Time Zone**.

Di seguito la procedura per la modifica di uno dei 16 profili preesistenti:

1. Selezionare il profilo che si intende modificare tramite il tasto di selezione **Edit** per visualizzare tutti i dettagli del profilo.

2. Modificare le impostazioni di preconfigurazione in modo che il profilo possa aderire alle esigenze dell'installazione.

Parametro	Descrizione
Name	Inserire il nome da assegnare al Time Slot.
Day	Spuntare i giorni di validità del Time Slot corrente (Sun=Domenica, Mon=Lunedi, Tue=Martedì, Wed=Mercoledì, Thu=Giovedì, Fri=Venerdì, Sat=Sabato)
Start Time	Indicare l'ora in cui attivare il Time Slot.
End Time	Indicare l'ora in cui disattivare il Time Slot.

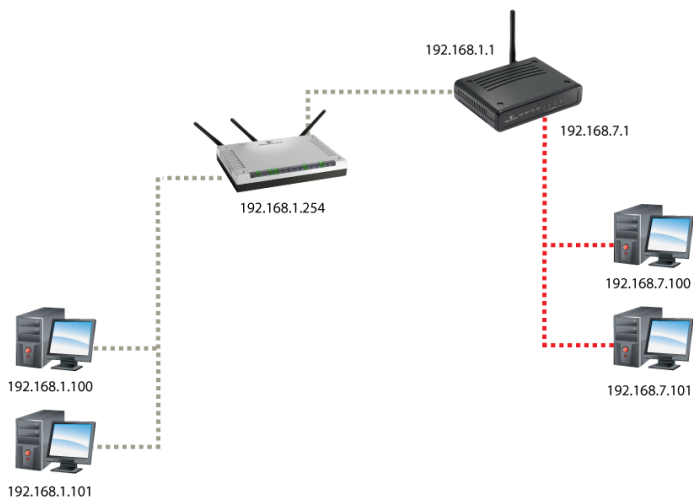
Premere il pulsante **Edit/Delete** per applicare le modifiche apportate.

Per cancellare una regola preesistente, selezionarla tramite il pulsante di selezione **Delete** e confermare l'operazione premendo il bottone **Edit/Delete**.

7.9 Advanced

In questa sezione, sarà possibile configurare alcune funzionalità dedicate al management avanzato del WebShare 3G 244WN, gli instradamenti statici e le Virtual Lan.

7.9.1 Static Route

Permette di configurare gli instradamenti statici nel caso in cui sia necessario effettuare routing all'interno della rete LAN.
Per comprendere al meglio questa funzionalità, ci serviremo di un esempio.
Si ponga di avere 2 segmenti di rete (192.168.1.0/24 ed 192.168.7.0/24), dove il dispositivo con indirizzo 192.168.1.100 appartente alla LAN del Router sia il responsabile dell'instradamento del traffico verso la rete 192.168.7.0/24.

Per poter raggiungere i client posti sulla sottorete 192.168.7.0/24, sarà necessario creare una regola di instradamento statico come segue:

Parametro	Descrizione
Destination	Indicare il segmento di rete o l'indirizzo IP da raggiungere.
Netmask	Indicare la maschera di rete relativa all'indirizzo dichiarato nel campo Destination.
Gateway	Inserire l'IP della macchina responsabile dell'instradamento dei pacchetti verso il segmento di rete da raggiungere.
Interface	Indicare l'interfaccia su cui instradare i pacchetti (Iplan nel caso di interfaccia LAN).
Cost	Introdurre il costo in HOP. Usualmente tale valore è 1. Mettere tale valore in funzione del numero di Router che è necessario attraversare per arrivare alla rete desiderata.

Premere su **Add** per aggiungere la regola di instradamento alla tabella di instradamento del Router.

Per cancellare una regola preesistente, selezionarla tramite il pulsante di selezione **Delete** e confermare l'operazione premendo il bottone **Edit/Delete**.

Per modificare una regola preesistente, selezionare la regola tramite il pulsante **Edit** ed eseguire le modifiche del caso; al termine, confermare le modifiche premendo il tasto **Edit/Delete**.

7.9.2 Static ARP

Questa sezione permette di configurare le associazioni ARP statiche nel caso in cui sia necessario che una particolare macchina (identificabile in maniera univoca tramite MAC Address) sia associata sempre allo stesso indirizzo IP.

Parametro	Descrizione
IP Address	Indicare l'indirizzo IP da associare al Mac Address indicato nel campo successivo
Mac Address	Indicare l'indirizzo MAC (nel formato xx:xx:xx:xx:xx:xx) al quale associare l'indirizzo IP indicato nel campo precedente.

Premere su **Add** per aggiungere l'associazione appena creata.

Per cancellare una regola preesistente, selezionarla tramite il pulsante di selezione **Delete** e confermare l'operazione premendo il bottone **Edit/Delete**.

Per modificare una regola preesistente, selezionare la regola tramite il pulsante **Edit** ed eseguire le modifiche del caso; al termine, confermare le modifiche premendo il tasto **Edit/Delete**.

7.9.3 Dynamic DNS

Tramite questa funzionalità è possibile registrare un dominio (del tipo nome dominio.dyndns.info) ed associarlo ad un IP dinamico. Ogni qual volta l'Adsl2+ si riconnetterà od effettuerà un rinnovo dell'indirizzo IP associate all'interfaccia WAN, tramite il client incorporato, comunicherà al server DNS il nuovo indirizzo IP assegnato dall'ISP. In questo modo, il Router ed i dispositivi ad esso collegati risulteranno sempre

raggiungibili (se non per brevi periodi di fail legati al tempo di aggiornamento dell'associazione IP/dominio); associando tale funzionalità con il Virtual Server è possibile:

- Gestire un server WEB interno alla proprio LAN
- Attivare un server FTP pubblico sul quale depositare materiale da condividere
- Controllare in maniera remota una macchina od un dispositivo collegati al Router (es: IPCamera, NAS oppure direttamente un PC tramite apposito software).

Per poter usufruire di tutti i vantaggi del servizio DynDns è necessaria l'attivazione di un account sul sito www.dyndns.org (per maggiori informazioni, fare riferimento all'appendice relativa).

Una volta registrato il dominio DynDns, è possibile associarlo al Router tramite il client integrato come da procedura indicata di seguito:

Parametro	Descrizione
Dynamic DNS	Attiva o disattiva il client DynDNS integrato.

Dynamic DNS Server	Indicare il provider di servizi DynDNS presso il quale si è precedentemente registrato un account DynDNS.
WildCard	Spuntare questa opzione per far si che anche i domini di livello inferiore vengano reindirizzati verso il client DynDNS (es: www.atlantis.dyndns.org)
Domain Name	Inserire il dominio registrato presso il provider di servizi DDNS.
Username	Inserire il nome utente utilizzato in fase di registrazione dell'account DDNS.
Password	Inserire la password utilizzata in fase di registrazione dell'account DDNS.
Period	Indicare il periodo (espresso in giorni) al termine del quale avrà luogo la sincronizzazione tra server e client.

Premere sul tasto **Apply** per confermare le impostazioni immesse.

A questo punto l'Adsl2+ Router è sempre e comunque raggiungibile dall'esterno. E' possibile ad esmpio ospitare un sito WEB o FTP (ruotando le opportune porte).
In questo modo ogni utente esterno interrogherà il server DDNS che gli restituirà di volta in volta l'indirizzo IP assegnato dall'ISP all' Adsl2+ Router. Usando la funzionalità di riconnessione (disponibile in PPPoA e PPPoE), qualora la connessione dovesse cadere, l' Adsl2+ Router la rialzerà immediatamente.

Atlantis Land consiglia di non impostare il campo Period con un valore superiore ai 25gg, in quanto in queste condizioni, l'indirizzo IP potrebbe essere considerato come statico, con conseguente disattivazione dell'account DynDNS.
Si consiglia inoltre di non procedere alla sincronizzazione client-server oltre le 3 volte al giorno, al fine di preservare il corretto stato di funzionamento del cliente integrato.

Al di là dell'intervallo impostato nel campo Period, il client integrato eseguirà la procedura di sincronizzazione col server ad ogni riconnessione del profilo PPP.
Si consiglia quindi di non utilizzare questa funzionalità in accordo con linee particolarmente rumoroso che potrebbero provocare eccessive richieste di sincronizzazione, con conseguente disattivazione dell'account.

7.9.4 Device Management

In questa sezione sarà possibile configurare le impostazioni relative alle modalità di management del WebShare 3G 244WN (SNMP, HTTP, etc).

La modifica di alcuni parametri di questa sezione richiedono un reboot dell'apparato per essere attivati. Questi parametri sono indicati con il simbolo (*).
Si ricorda che rendere definitive le configurazione anche dopo il reboot dell'apparato, è necessario che le stesse vengano salvate su memoria non volatile (ROM), tramite la pressione del tasto **Save Config To Flash**.

Device Management		
Device Host Name		
Host Name	home.gateway	
Embedded Web Server		
* HTTP Port	80	(80 is default HTTP port)
Management IP Address	0.0.0.0	('0.0.0.0' means Any)
Management IP Netmask	255.255.255.255	
Management IP Address(2)	0.0.0.0	
Management IP Netmask(2)	255.255.255.255	
Expire to auto-logout	180	seconds
Universal Plug and Play (UPnP)		
UPnP	◉ Enable ○ Disable	
* UPnP Port	2800	
SNMP Access Control		
SNMP	◉ Enable ○ Disable	

Device Host Name

Parametro	Descrizione

Host Name	Inserire il nome con il quale il WebShare 3G 244WN verrà visto dalle periferiche di rete.

Embedded Web Server

Parametro	Descrizione
HTTP Port	Inserire il numero di porta servizio da utilizzare per il management web del dispositivo.
Management IP Address	Inserire l'indirizzo IP abilitato all'accesso all'interfaccia di configurazione del prodotto (nel caso in cui si desideri che qualsiasi indirizzo IP possa avere accesso all'interfaccia, impostare il campo con valore 0.0.0.0)
Management IP Netmask	Inserire la maschera di rete relativa al campo Management IP Address (nel caso in cui si desideri che il solo IP indicato nel campo Management IP Address sia abilitato all'accesso, impostare il campo con valore 255.255.255.255)
Management IP Address (2)	Inserire l'indirizzo IP abilitato all'accesso all'interfaccia di configurazione del prodotto (nel caso in cui si desideri che qualsiasi indirizzo IP possa avere accesso all'interfaccia, impostare il campo con valore 0.0.0.0)
Management IP Netmask (2)	Inserire la maschera di rete relativa al campo Management IP Address (nel caso in cui si desideri che il solo IP indicato nel campo Management IP Address sia abilitato all'accesso, impostare il campo con valore 255.255.255.255)
Expire to Auto-logout	Impostare l'intervallo al termine del quale verrà attivata la procedura di logout per l'utente abilitato alla configurazione del prodotto.

Universal Plug'n'Play (UP'n'P)

Parametro	Descrizione
UPnP	Abilita o disabilita il supporto Universal Plug'n'Play. Questa tecnologia permette, se supportata dall'applicazione, la creazione di regole dinamiche di port-forwarding in modo da garantire il corretto funzionamento dell'applicativo utilizzato (es: Windows Live Messenger).
UPnP Port	Impostare la porta servizio per la gestione delle comunicazione UPnP tra i dispositive di rete ed il Router. Si consiglia vivamente di mantenere la porta predefinita al fine di evitare conflitti.

SNMP Access Control			
SNMP	◉ Enable ○ Disable		
SNMP V1 and V2			
Read Community	public	IP Address	0.0.0.0
Write Community	password	IP Address	0.0.0.0
Trap Community		IP Address	
SNMP V3			
Username		Password	
Access Right	◉ Read ○ Read/Write	IP Address	

** : This setting will become effective after you save to flash and restart the router.*
** : When you enable remote access, please disable/enable the remote access to update the HTTP port.*

Apply

SNMP Access Control

Parametro	Descrizione
SNMP	Abilita o disabilita il client SNMP per l'interfacciamento del Router con strumenti di log esterni.

SNMP V1 and V2

Parametro	Descrizione
Read Community	Specificare il nome per identificare la Read Community (e l'indirizzo IP da cui si può accedere). E' una sorta di password che il dispositivo controlla prima di concedere l'acesso in lettura dei dati.
Write Community	Specificare il nome per identificare la Write Community (e l'indirizzo IP da cui si può accedere). E' una sorta di password che il dispositivo verifica prima di poter accedere alla configurazione.
Trap Community	Specificare un nome per identificare una Trap Community e un indirizzo IP cui verrano inviate le Trap.

SNMP V3

Parametro	Descrizione
Username	Inserire il nome utente per l'autenticazione dell'account SNMP.
Password	Inserire la password per l'autenticazione dell'account SNMP.
Access Right	Impostare i diritti di lettura o lettura/scrittura per l'account SNMP.

Il campo Host Name non può essere compost da una sola parola. Di seguito un esempio di sintassi:

Host Name: homegateway ==> **Incorrect**
Host Name: home.gateway or my.home.gateway ==> **Correct**

WebShare 3G 244WN supporta le seguenti MIBs:

RFC 1213 (MIB-II):
System group
Interfaces group
Address Translation group
IP group
ICMP group
TCP group
UDP group
EGP (not applicable)
Transmission
SNMP group

RFC1650 (EtherLike-MIB):
dot3Stats

RFC 1493 (Bridge MIB):
dot1dBase group
dot1dTp group
dot1dStp group (if configured as spanning tree)

RFC 1471 (PPP/LCP MIB):

pppLink group
pppLqr group (not applicable)

RFC 1472 (PPP/Security MIB):
PPP Security Group)

RFC 1473 (PPP/IP MIB):
PPP IP Group

RFC 1474 (PPP/Bridge MIB):
PPP Bridge Group

RFC1573 (IfMIB):
ifMIBObjects Group

RFC1695 (atmMIB):
atmMIBObjects

RFC 1907 (SNMPv2):
only snmpSetSerialNo OID

7.9.5 IGMP

Tradizionalmente i pacchetti IP vengono trasmessi in Unicast (1 trasmittente – 1 ricevente) oppure in Broadcast (1 trasmittente – tutta la rete). Il Multicast permette di inviare pacchetti ad un gruppo definito di hosts sulla rete.
L'IGMP (Internet Group Multicast Protocol) è un protocollo utilizzato per stabilire una relazione di appartenenza in un gruppo Muticast – non è utilizzato per trasportare dati dell'utenza. L'IGMP versione 2 (RFC 2236) è un'implementazione perticolare della versione 1 (RFC 1112) che resta ancora largamente utilizzata. Per maggiori dettagli sull'interoperabilità tra i protocolli IGMP versione 1 e 2 è possibile consultare le sezioni 4 e 5 dell' RFC 2236. Gli indirizzi IP di classe D sono utilizzati per identificare un gruppo di hosts e si trovano nel range da 224.0.0.0 a 239.255.255.255.
L'indirizzo IP 224.0.0.0 non è assegnato ad alcun gruppo, è utilizzato da computers con IP Multicast. L'indirizzo 224.0.0.1 è utilizzato per messaggi di richiesta ed è assegnato al gruppo permanente di tutti gli indirizzi IP (inclusi i gateways). Tuti gli

hosts devono appartenere al gruppo 224.0.0.1 per partecipare alla comunicazione IGMP. L'Adsl2+ VPN Router supporta entrambe le versioni del protocollo IGMP. Allo Start-Up il Router interroga tutte le reti a lui direttamente connesse per identificare le appartenenze ai gruppi.
Fatto ciò, il Router aggiorna periodicamente queste informazioni.

Parametro	Descrizione
IGMP Forwarding	Permette l'accettazione di pacchetti multi cast.
IGMP Snooping	Permette alle porte Ethernet la verifica e la decisione di una poltica di instradamento corretta.

7.9.6 VLAN Bridge

Tramite questa sezione sarà possibile associare le differenti interfaccie bridge (fare riferimento al capitol specifico), a differenti VLAN.

Parametro	Descrizione
Edit	Permette di modificare le porte membro della VLAN selezionata.
Create VLAN:	Permette la creazione di una nuova VLAN.

7.10 Language

Permette di selezionare la lingua relativamente all'interfaccia di configurazione tra Inglese e Francese.

8. Save Config, Restart e Logout

Grazie ai pulsanti Save Config, Restart e Logout sarà possibile gestire in maniera immediate il salvataggio permanente della configurazione su memoria non volatile, riavviare il prodotto oppure effettuare il logout dell'utente dall'interfaccia di configurazione.

Si ricorda che al fine di salvare in maniera permanente le configurazioni all'interno del WebShare 3G 244WN, è necessario salvare le stesse in una parte di memoria statica (ROM).
Premere il tasto **Save Config** al termine della configurazione per scrivere i parametri impostati all'interno della memoria fissa.
La mancata adozione di questa procedura comporterà l'inevitabile perdita di tutti i dati di configurazione al riavvio del dispositivo.

APPENDICE A: Avvertente per utilizzo con abbonamenti a consumo

WebShare 3G 244WN, come molti dei dispositivi Modem/Router ad oggi in commercio, è stato sviluppato per permettere l'accesso Internet a un'intera LAN di PC.
Al fine di garantire la condivisione di un solo abbonamento ADSL tra più PC, il dispositivo si sostituisce al PC, prendendo in carico tutta la fase di negoziazione della connessione con la centrale ADSL; in questo caso quindi, a differenza di un semplice modem, è il dispositivo stesso ad essere realmente connesso alla rete Internet e non i singoli PC a lui collegati.
Grazie alla tecnologia di connessione Always On, il Router è progettato per mantenere sempre attiva la connessione Internet, con un importante aggravio dei costi se utilizzato con abbonamenti non FLAT (e quindi con tariffazione a tempo/pacchetto).
Su quest'ultima tipologia di linee ADSL non è difatti consigliato l'utilizzo di un router, in quanto non è possibile gestire direttamente la connessione/disconnessione dell' apparato dal uno dei terminali ad esso collegati.
In questa situazione si consiglia vivamente di spegnere il router ADSL oppure scollegare il cavo di linea ADSL dell'apparato quando non si necessita della connessione a Internet.
Si ricorda che WebShare 3G 244WN può comunque essere configurato in modalità Connect On Demand, in modo tale che, se l'apparato non rilevasse traffico dati verso Internet per un determinato periodo di tempo, il dispositivo abbatta automaticamente la connessione logica con la centrale (lo spegnimento del led Internet indica la non connessione con la centrale ADSL).

Pur avendo tutti i presupposti per essere una valida alternativa a quanto detto sopra, questa modalità di connessione mostra comunque alcune debolezze di cui è bene tenere conto:

- Per riattivare la connessione è sufficiente che un PC effettui una richiesta dati verso Internet. Una volta rilevata questa richiesta, il router ADSL effettua in automatico una nuova connessione a Internet.
- Alcuni programmi recenti, sviluppati in seguito all'avvento delle connessioni a banda larga, effettuano degli aggiornamenti periodici automatici su Internet. È questo il caso, ad esempio, degli antivirus, dei server DNS, di MSN Messenger e altri ancora.

A fronte di queste considerazioni è possibile che WebShare 3G 244WN, nel caso in cui tali programmi non vengano configurati in maniera opportuna, possa collegarsi a Internet varie volte per periodi prolungati, a totale insaputa dell'utente, con conseguente tariffazione da parte dell'operatore, del costo della navigazione.
È per questi motivi che tutte le case produttrici di router ADSL consigliano di spegnere il dispositivo quando non è necessario l'utilizzo della connettività.

APPENDICE B: Troubleshooting

Questo capitolo illustra come identificare e risolvere eventuali problemi sul WebShare 3G 244WN .

A.1 Utilizzare i LED per la diagnosi dei problemi

I LEDs sono un utile strumento per individuare eventuali problemi, osservandone lo stato è possibile individuare velocemente dove si verifica un eventuale malfunzionamento.

A.1.1 LED Power

Il LED PWR non si accende

Steps	Azione Correttiva
1	Accertarsi che l'alimentatore sia connesso al WebShare Router ed alla rete elettrica. Utilizzare unicamente l'alimentatore fornito a corredo.
2	Verificare che l'alimentatore sia connesso a una presa elettrica attiva e in grado di fornire la tensione necessaria al funzionamento del prodotto. Accertarsi che il bottone di accensione, posto sul retro, sia su ON.
3	Accertarsi che il Plug dell'alimentatore sia correttamente inserito.
4	Se il problema persiste contattare l'assistenza tecnica Atlantis Land.

A.1.2 LED LAN

Il LED LAN non si accende.

Steps	Azione Correttiva
1	Verificare la connessione del cavo di rete tra il router e il PC o lo

	Switch di rete.
2	Verificare che il cavo sia funzionante.
3	Verificare che la scheda di rete del PC funzioni correttamente.
4	Se il problema persiste contattare l'assistenza tecnica Atlantis Land.

A.1.3 LED ADSL

Il LED ADSL non si accende e/o lampeggia continuamente.

Steps	Azione Correttiva
1	Verificare che il cavo telefonico e la presa a muro funzionino correttamente.
2	Verificare che il Provider abbia attivato il servizio ADSL.
3	Reinizializzare la linea ADSL impostando il protocollo utilizzato dal'ISP (Configuration, WAN, ADSL Mode).
4	Se il problema persiste contattare l'assistenza tecnica Atlantis Land.

A.2 Telnet

Non è possible accedere al WebShare 3G 244WN tramite il servizio Telnet.

Steps	Azione correttiva
1	Verificare la connessione del cavo di rete tra il router e il PC o lo Switch di rete.
2	Accertarsi di utilizzare un indirizzo IP corretto, appartenente alla stessa rete del WebShare Router .
3	Eseguire un ping verso il WebShare 3G 244WN. Se l'esito è negativo verificare l'indirizzo IP del PC, se si utilizza il servizio DHCP verificare che il sistema abbia ricevuto correttamente le impostazioni di rete.
4	Accertarsi di aver inserito correttamente la password, l'impostazione di default è **atlantis**. Se la password è stata dimenticata fare riferimento alla sezione opportuna.
5	Verificare che nella sezione **Firewall -> Packet Filter** sia consentito il servizio Telnet dall'interfaccia/indirizzo dal quale si sta tentando l'accesso al prodotto.
6	Se il problema persiste contattare l'assistenza tecnica Atlantis

	Land.

A.3 Configurazione WEB

Non è possible accedere all'interfaccia Web di configurazione.

Steps	Azione correttiva
1	Accertarsi di utilizzare un indirizzo IP corretto, appartenente alla stessa rete del WebShare Router.
2	Accertarsi di non avere una sessione Console attiva.
3	Accertarsi nella sezione **Configuration -> Advanced -> Device Management** di aver abilitato per l'indirizzo IP della macchina l'accesso Web per la configurazione (Management IP Address). Verificare inoltre che il traffico HTTP verso l'interfaccia LAN del Router non sia inibito dal Firewall (**Firewall -> Packet Filter**).
4	Per l'accesso dalla WAN è necessario abilitare il servizio attraverso la voce **System -> Remote Management**. Per rendere permanente questa tipologia di accesso, sarà necessario creare un'opportuna regola di Virtual Server che reindirizzi la porta TCP 80 verso l'indirizzo IP 192.168.1.254
5	Asscurarsi di utilizzare le credenziali di accesso corrette. Quelle di default sono username=**admin**, password=**atlantis**. Nel caso in cui siano state modificate in fase di configurazione e non si abbia modo di reperire le stesse, è possibile eseguire un ripristino alle condizioni di fabbrica. Per ulteriori approfondimenti fare riferimento al paragrago **Impostazioni di fabbrica**.
6	Verificare che un altro utente non sia temporaneamente loggato con privilegi amministrativi. WebShare 3G 244WN supporta una sola sessione di management per volta.
7	Accertarsi che la porta di configurazione del prodotto non sia stata variata per esigenze di rete. E' possibile verificare questo valore nel menù **Configuration –> Advanced -> Device Management**. Nel caso sia stata variata, assicurarsi che la sintassi dell'indirizzo sia http://x.y.z.k:numeroporta.
8	Fare riferimento anche alla sezione ***A.8.***

Le schermate di configurazione Web non vengono visualizzate correttamente.

Steps	Azione correttiva
1	Accertarsi che il browser utilizzato per la configurazione sia compatibile. I browser testati al momento della stesura del documento sono Internet Explorer (v6, 7, 8) e Mozilla Firefox.
2	Eliminare i files temporanei e l'eventuale cache del browser. Al termine effettuare una nuova procedura di login
3	Alcuni browser supportano algoritmi nativi per garantire la compatibilità con piattaforme realizzate su tecnologie precedenti. Verificare e nel caso disabilitare questa tipologia di funzionalità.

A.4 Login con Username e Password

E' stata dimenticata la password di accesso.

Steps	Azione correttiva
1	Se è stata cambiata la password di accesso ed è stata dimenticata, sarà necessario caricare la configurazione di default. Ciò cancellerà tutte le configurazioni eseguite dall'utente e ripristinerà la password di default. Premendo il pulsante **Reset** presente nel pannello posteriore del prodotto per 10 (o più) secondi, il router riporterà tutte le impostazioni ai valori iniziali (il tasto SYS si spegnerà per indicare l'avvenuto reset, comincerà a lampeggiare segnalando il caricamento del firmware e poi diventerà fisso).
2	I parametri di default per l'accesso alla configurazione del Router ADSL sono: Username: **admin** Password: **atlantis**
3	Per incrementare il livello di sicurezza del sistema è molto importante modificare la password di default.

A.5 Interfaccia LAN

Non è possible accedere al WebShare 3G 244WN dalla LAN e nemmeno eseguire un ping dal router verso i PC della rete.

Steps	Azione correttiva
1	Verificare che i LEDs relativi alle porte LAN posti sul pannello

	frontale del WebShare 3G 244WN siano accesi in corrispondenza dei cavi di rete collegati. Se entrambi i LEDs sono spenti fare riferimento alla sezione A.1.2.
2	Accertarsi di utilizzare un indirizzo IP corretto, appartenente alla stessa rete del WebShare 3G 244WN. Nel caso si prega di fare riferimento al paragrafo dedicato alla configurazione dei client contenuto in questo documento.
3	Se è stato modificato l'indirizzo IP lato LAN del Router ADSL oppure la porta di comunicazione, è necessario modificare L'URL di accesso al prodotto secondo la sintassi http://x.y.z.k:numeroporta
4	Verificare che la porta alla quale si è collegati non sia appartenente ad un interfaccia VLAN differente dalle altre e non abilitata al management del prodotto. Nel caso in cui non sia possibile verificare questa condizione, effettuare un reset dell'apparato.
5	Se i problemi persistono, effettuare un reset dell'apparato.

Non è possibile utilizzare la tecnologia Gigabit Ethernet per la comunicazione tra il Router ed il PC.

Steps	Azione correttiva
1	Verificare che i LEDs relativi alle porte LAN posti sul pannello frontale del WebShare 3G 244WN siano accesi in corrispondenza dei cavi di rete collegati. Se entrambi i LEDs sono spenti fare riferimento alla sezione A.1.2.
2	Verificare la tipologia del cavo di rete utilizzato per la connessione. Si ricorda che per poter usufruire della tecnologia Gigabit è necessario utilizzare un cavo a 4 coppie CAT.5 o superiore.
3	Verificare che la NIC installata sul PC supporti la modalità Gigabit Ethernet e sia correttamente configurata. Nel caso, è possibile forzare la negoziazione della velocità impostando il valore 1000Mbps manualmente.
4	Verificare tramite la sezione **Configuration -> LAN -> Port Setting** che la porta relativa sia configurata in modalità **Auto**. Nel caso è possibile forzare la modalità di connessione manualmente.

A.6 Interfaccia WLAN

Il client wireless, configurato in DHCP, non riceve l'indirizzo IP dal router.

Steps	Azione correttiva
1	Accertata l'avvenuta connessione con la WLAN del router, provare ad aggiornare i driver del client wireless.
2	Se il problema persistesse, procedere come da punto 3 per impostare un indirizzo IP statico ai vari client. Talune volte infatti il pacchetto DHCP non riesce a passare a cause di settaggi **RTS/CTS** e **Fragmentation Threshold(bytes).**
3	Assegnare al client Wireless un indirizzo IP statico (del tipo 192.168.1.1, subnet=255.255.255.0, DG=192.168.1.254) e provare ad effettuare un ping verso l'indirizzo IP del router.

A.7 Interfaccia WAN

L'inizializzazione della connessione ADSL fallisce.

Steps	Azione correttiva
1	Verificare che il cavo telefonico e la presa a muro funzionino correttamente. Il LED ADSL dovrebbe essere acceso.
2	Nel caso di allineamento difficoltoso, potrebbe essere necessario forzare la modulazione utilizzata dal modulo ADSL tramite la sezione **Configuration -> ADSL Mode**.
3	Verificare che i valori di VPI e VCI siano corretti, nel dubbio verificare tali parametri con il proprio Provider.
4	Riavviare il Router ADSL. Se il problema persiste contattare l'assistenza tecnica Atlantis Land.

Non è possibile utilizzare la connessione 3G tramite il modem collegato alla porta USB.

Steps	Azione correttiva
1	Verificare la compatibilità del modem utilizzato con la lista di compatibilità presente alla fine di questo documento. Una versione aggiornata della lista è reperibile presso il sito www.atlantis-land.com alla relativa sezione di prodotto.
2	Verificare che la SIM card utilizzata non sia protetta da PIN e nel caso inserire il PIN all'interno dei parametri di configurazione tramite

	la pagina **Configuration -> WAN -> WAN Profile**.
3	Verificare la copertura di rete tramite la finestra **Status -> 3G Status**.
4	Verificare la corretta configurazione del profilo di connessione in accordo con l'offerta del proprio operatore mobile. Una lista dei parametri relativi ai principali ISP italiani è riportata al termine di questo documento.

Non è possibile ottenere un indirizzo IP pubblico dall' ISP.

Steps	Azione correttiva
1	L' indirizzo IP pubblico viene fornito dal Provider dopo l'autenticazione di username e password.
2	Questo tipo di autenticazione si verifica solo con i protocolli PPPoE e PPPoA, verificare quindi che i parametri inseriti siano corretti.
3	In caso di connessioni 3G, fare riferimento al punto precedente.

A.8 Accesso ad Internet

Non è possibile accedere ad Internet.

Steps	Azione correttiva
1	Accertarsi che il Router ADSL sia stato impostato correttamente per la connessione ad Internet. Nel caso in cui si utilizzi un abbonamento di tipo PPPoA/PPPoE, lo stato del led PPP indicherà il corretto funzionamento della connessione.
2	Verificare ed eventualmente disabilitare temporaneamente software Firewall e/o Antivirus al fine di verificare eventuali blocchi da parte di questi ultimi.
2	Se il LED ADSL è spento fare riferimento alla sezione A.1.3.

La connessione ad Internet si disconnette.

Steps	Azione correttiva
1	Verificare le impostazioni di scheduling della connessione.
2	Se si utilizzano i protocolli PPPoA e PPPoE per la connessione verificare le impostazioni di IDLE-TIMEOUT.
3	Verificare che il valore di SNR (Status-Downstream) sia almeno

	12dB.
4	Contattare l'ISP.

A.9 Amministrazione Remota

Non è possibile amministrare il WebShare 3G 244WN dalla LAN o dalla WAN.

Steps	Azione correttiva
1	Accedere alla pagina **Configuration -> Advanced -> Device Management** ed impostare nel campo IP Management l'indirizzo IP da utilizzare per l'amministrazione del prodotto.
2	Verificare la presenza di regole di Firewall attraverso la sezione **Configuration -> Firewall -> Packet Filter** che potrebbero inibire l'accesso al Router.
3	Utilizzare l'indirizzo IP pubblico per accedere alla configurazione del Router ADSL dalla WAN. Utilizzare l'indirizzo IP privato per accedere alla configurazione del Router ADSL dalla LAN.
4	Fare riferimento alla sezione ***A.5*** per verificare la connessione alla LAN. Fare riferimento alla sezione ***A.6*** per verificare la connessione alla WLAN. Fare riferimento alla sezione ***A.7*** per verificare la connessione alla WAN.
5	Fare riferimento anche alla sezione ***A.4.***

A.10 Varie

La navigazione avviene senza problemi ma le prestazioni di Emule (programmi di p2p) non sono soddisfacenti (attribuzione di un ID basso).

Steps	Azione correttiva
1	Accedere via WEB al Router, cliccare su **Configuration –> Virtual Server** e creare 2 regole come in figura.

Rule	Application	Protocol	Start Port	End Port	Local IP Address
1	-Emule TCP	TCP	13333	13333	192.168.1.1
2	-Emule UDP	UDP	59052	59052	192.168.1.1

Si è assunto che il PC su cui giri Emule abbia indirizzo IP 192.168.1.1 (statico

	e non ottenuto tramite DHCP) e che Emule usi le porte TCP 13333 ed UDP 59052.
2	Verificare che Emule (la procedura va bene per qualsiasi altro software) usi effettivamente le porte di sopra. Atlantis Land non potrà fornire supporto (sulle porte utilizzate) che andrà richiesto al produttore del software in questione.
3	Contattare il proprio Internet Service Provider e verificare che non siano presenti blocchi particolari per i programmi di p2p.

A.11 Wireless

Domanda	Risposta
Posso avviare un' applicazione da un computer remoto presente sulla rete wireless?	Questo dipende direttamente dall'applicazione stessa, se è stata progettata per lavorare in rete (non fa differenza che sia wireless o cablata) non ci sarà alcun problema.

Domanda	Risposta
Posso giocare in rete con gli altri computer presenti sulla WLAN?	Si, se il gioco è dotato di funzionalità multiplayer in rete.

Domanda	Risposta
Cos'è lo Spread Spectrum?	La trasmissione Spread Spectrum si basa sulla dispersione dell'informazione su una banda molto più ampia di quella necessaria alla modulazione del segnale disponibile. Il vantaggio che si ottiene da questa tecnica di modulazione è infatti una bassa sensibilità ai disturbi radioelettrici anche per trasmissioni a potenza limitata. Questa caratteristica è ovviamente preziosa quando si devono trasmettere dei dati.

Domanda	Risposta
Cosa sono DSSS e FHHS?	DSSS (Direct-Sequence Spread-Spectrum): E' una particolare tecnologia di trasmissione per la banda larga che consente di

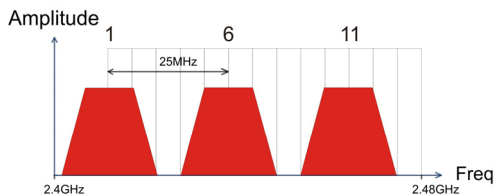
	trasmettere ogni bit in maniera ridondante. E' adatta in particolare per la trasmissione e la ricezione di segnali deboli. FHHS (Frequency Hopping Spread Spectrum): è una tecnologia che permette la condivisione tra più utenti di uno stesso insieme di frequenze. Per evitare interferenze tra periferiche dello stesso tipo le frequenze di trasmissione cambiano sino a 1.600 volte ogni secondo.

<table>
<tr><th>Domanda</th><th>Risposta</th></tr>
<tr><td>Cos'è un decibel?</td><td>Il deciBel è un'unita misura relativa che esprime un rapporto fra 2 valori. E' importante sottolineare che è adimensionale (non si misura in watt) e permette di capire immediatamente lo scostamento dalla misura campione o riferimento. E' utilizzato perché permette di avere un'immediata percezione della differenza di 2 misurazioni, essendo il logaritmo una misura compressa e non lineare.
L'equazione canonica è la seguente: dB = 10 log10 (P 2 / P 1). Dove P1 è la misura riferimento e P 2 è la misura istantanea.</td></tr>
<tr><td>dBm</td><td>Definiamo il dBm=10 log 10 (P 2 / P 1), dove P1 =1 milliWatt (mW).
E' possibile pertanto parlare di potenza trasmessa sia utilizzando il watt che il dBm.
Nella tabella seguente è riportata l'equivalenza per i valori più comuni (utilizzare la formula di sopra per valori non in tabella):
<table>
<tr><td>dBm</td><td>Watt</td><td>note</td></tr>
<tr><td>0</td><td>1 mW</td><td></td></tr>
<tr><td>3</td><td>2 mW</td><td></td></tr>
<tr><td>6</td><td>4 mW</td><td></td></tr>
<tr><td>9</td><td>8 mW</td><td></td></tr>
<tr><td>10</td><td>10 mW</td><td></td></tr>
<tr><td>12</td><td>15,8 mW</td><td></td></tr>
</table></td></tr>
</table>

<table>
<tr><td></td><td>
<table>
<tr><td>13</td><td>20 mW</td><td></td></tr>
<tr><td>14</td><td>25 mW</td><td></td></tr>
<tr><td>15</td><td>32 mW</td><td></td></tr>
<tr><td>16</td><td>40 mW</td><td></td></tr>
<tr><td>17</td><td>50 mW</td><td></td></tr>
<tr><td>18</td><td>63 mW</td><td></td></tr>
<tr><td>19</td><td>79 mW</td><td></td></tr>
<tr><td>20</td><td>100 mW</td><td>Massima Potenza utilizzabile per WLAN a 2.4Ghz</td></tr>
<tr><td>23</td><td>200 mW</td><td></td></tr>
<tr><td>26</td><td>400 mW</td><td></td></tr>
<tr><td>29</td><td>800 mW</td><td></td></tr>
</table>
</td></tr>
<tr><td>dBi</td><td>Il guadagno di un'antenna è definito come il rapporto fra la densità di potenza irradiata dall'antenna in esame nella direzione di massima direttività (P 2) e la densità di potenza che irradierebbe un'antenna isotropa alimentata con la stessa potenza.
Definiamo il dBi=10 log 10 (P 2 / P isotropica),

dBm=10 log 10 (Potenza/ 1mW)</td></tr>
<tr><td>Antenna Isotropica</td><td>Il deciBel è un’unita misura relativa che esprime un rapporto fra 2 valori. E’ importante sottolineare che è adimensionale (non si misura in watt) e permette di capire immediatamente lo scostamento dalla misura campione o riferimento. E’ utilizzato perché permette di avere un’immediata percezione della differenza di 2 misurazioni, essendo il logaritmo una misura compressa e non lineare.
L’equazione canonica è la seguente: dB = 10 log10 (P 2 / P 1). Dove P1 è la misura riferimento e P 2 è la misura istantanea.</td></tr>
<tr><td>Antenna Direttiva</td><td>Il guadagno di un'antenna è definito come il rapporto fra la potenza irradiata dall'antenna in esame nella direzione di massima direttività e la potenza
che irradierebbe un'antenna isotropa alimentata con la stessa potenza.</td></tr>
</table>

Interferenze sulla WLAN?

Domanda	Risposta
Banda ISM	Questa frequenza è stata messa a disposizione dalla FCC, su richiesta delle aziende che intendevano sviluppare soluzioni wireless per l'uso civile quotidiano ed è generalmente contraddistinta dalla sigla ISM band (Industrial, Scientific and Medical). In questa frequenza operano solo dispositivi industriali, scientifici e medici a basse potenze.
Come posso eliminare le interferenze che deteriorano le prestazioni della WLAN?	Anzitutto spegnere (o allontanare) ogni dispositivo che operi nelle stesse frequenze. Utilizzare antenne direzionali per far "imbarcare" meno rumore ai dispositivi. In caso si altri AP adiacenti consultare la faq sull'assegnazione dei canali.
Canali	Ogni canale occupa all'incirca 22Mhz, essendo l'intera banda ISM di 80Mhz possono essere utilizzati contemporaneamente soltanto 3 dei 13 canali disponibili. E' consigliabile mantenere una distanza di 5 canali tra due utilizzati (es. AP1-canale 1, AP2-canale 6). L'interferenza si verifica quando due o più canali si sovrappongono degradando le prestazioni, questa sovrapposizione è chiamata "**Overlap**". Il disegno seguente illustra meglio quanto detto:

Sino a 3 AP possono coesistere senza overlapping. E' opportuno prestare attenzione all'assegnazione dei canali.

Domande Varie ?

Domanda	Risposta
WDS	Il WDS (Wireless Distribution System) è la tecnologia che permette ad un Access Point di svolgere contemporaneamente la funzionalità di AP e di Repeater del segnale. Risulta essere la soluzione ottimale per estendere la copertura di una wireless LAN in ambienti dove non è assolutamente possibile stendere cavi. Può essere utile per raggiunge relocazioni remote. Va osservato che l'uso di un repeater ha un forte impatto sulle prestazioni dei client wireless ad esso collegati. Apparati che supportano tale tecnologia, a listino Atlantis land sono: A02-AP1-W54 A02-AP1-W54PoE A02-RA242-W54
IEEE802.11g	Il nuovo standard 802.11g opera alla frequenza di 2,4 GHz e quindi è pienamente compatibile con la più diffusa versione b. Il vantaggio è che consente una velocità di trasferimento di 54 Mbps, cinque volte superiore allo standard 802.11b.
Infrastructure	Nella configurazione Infrastructure una rete WLAN e una rete WAN comunicano tra loro tramite un access point.

Sicurezza	L’Access Point offre funzionalità di crittografia WEP fino a 128 bit, ciò provvede a rendere sicure le trasmissioni dati wireless. L’utilizzo del WPA e/o WPA2 rende ancora più sicura la trasmissione wireless. Tali tecnologie devono essere supportate anche dai vari client utilizzati.

APPENDICE C: MultiNat

Grazie a questa funzionalità è possibile gestire più interfacce LAN. Solitamente la tipologia di contratti offerti dall'ISP ricade entro una delle seguenti tipologie:

- A=1 Indirizzo IP Dinamico, in genere offerto con PPPoA/PPPoE
- B=1 Indirizzo IP statico, in genere offerto con RFC1483 Routed
- C=N Indirizzi IP statico, in genere offerto con RFC1483 Routed

Solitamente la punto-punto è routata e pubblica. N è un multiplo di 8.

In figura sono riportate le possibili configurazioni del Router:

Tipo Abbonamento	WAN	LAN	IP Alias	Note
1 Indirizzo IP statico **(Tipo A)**	Va configurata con i dati della punto-punto con NAT attivo.	Va configurata con una classe privata che verrà nattata sull'IP pubblico della WAN.	N/A	
N indirizzi IP statici **(Tipo B)**	Va configurata con i dati della punto-punto con NAT Non attivo.	Va configurata con la classe pubblica. In questo caso al LAN IP del router si assegna uno degli N IP ed ai PC gli altri N-3.	Non configurato	Facile Configurazione Possono Navigare solo N-3 PC con IP pubblico.
N indirizzi IP	Va	Va	Si configura	Configurazione

statici **(Tipo B)**	configurata con i dati della punto-punto con NAT attivo.	configurata con una classe privata che verrà nattata sull'IP pubblico della WAN.	il Router con uno degli N IP della classe pubblica ed ai PC gli altri N-3. In totale i PC che potranno navigare con IP pubblico sono N-3. L'interfaccia è di tipo External.	non immediata Possono Navigare N-3 PC con indirizzo pubblico e quanti PC si vogliono dietro il NAT della punto-punto. Attenzione la punto-punto deve essere routata e pubblica.

Segue nel dettaglio la configurazione dell'ultimo caso (TIPO **C**).
Per ipotesi il contratto con l'ISP sia il seguente:

Punto-Punto Routata Pubblica

- IP Lato Router=80.80.80.214
- Defaukt Gateway=80.80.80.213
- Subnet Mask=255.255.255.252

Classe di 8 IP Pubblici

- 8 IP, il cui primo è 81.38.28.64
- subnet 255.255.255.248

La configurazione procede nei seguenti passi:

1) Configurazione della WAN: Scegliere RFC1483 Routed impostando l'incapsulazione in LLC Routed. Introdurre poi i dati della punto-punto.

2)La parte LAN del Router: può essere lasciata come da default sull'IP 192.168.1.254 o comunque su una classe privata. Tutti i PC appartenenti a questa classe e con default Gateway l'IP del Router avranno accesso ad internet sull'IP WAN della Punto-Punto.

3)Sezione IP Alias: Accedere alla sezione **Configuration**, poi **LAN** ed infine **IP Alias.** Cliccare su Add ed introdurre la classe pubblica come in figura (scegliere **external** il tipo di interfaccia).

Si ricorda che il primo e l'ultimo IP non vanno utilizzati (nel caso in esame 81.38.28.64 e 81.38.28.71). Assegnare di norma un IP (il primo se non espressamente precisato dall'ISP) all'interfaccia IP Alias esterna del Router.
In questo caso assegnare al primo PC il seguente indirizzo=81.38.28.66, subnet=255.255.255.248 e default gateway=81.38.28.65. Tale PC avrà un IP pubblico (non nattato). E' possibile far navigare in questo modo sino a 5 PC o apparati diversi.

In Figura un dettaglio della configurazione della rete:

Host	Indirizzo IP	Maschera	Gateway	DNS
Router Lan IP Alias	81.38.28.65	255.255.255.248		
PC 1 (pubblico)	81.38.28.66	255.255.255.248	81.38.28.65	Forniti ISP
PC 2 (pubblico)	81.38.28.67	255.255.255.248	81.38.28.65	Forniti ISP
PC 3 (pubblico)	81.38.28.68	255.255.255.248	81.38.28.65	Forniti ISP
PC 4 (pubblico)	81.38.28.69	255.255.255.248	81.38.28.65	Forniti

				ISP
PC 5 (pubblico)	81.38.28.70	255.255.255.248	81.38.28.65	Forniti ISP
Router Lan IP	192.168.1.254	255.255.255.0		
PC 1 (privato)	192.168.1.1	255.255.255.0	192.168.1.254	Forniti ISP
PC 2 (privato)	192.168.1.2	255.255.255.0	192.168.1.254	Forniti ISP
PC 3 (privato)	192.168.1.3	255.255.255.0	192.168.1.254	Forniti ISP
PC 4 (privato)	192.168.1.4	255.255.255.0	192.168.1.254	Forniti ISP
PC n (privato)	192.168.1.N	255.255.255.0	192.168.1.254	Forniti ISP
Router WAN IP (NAT attivo)	81.40.14.214	255.255.255.252	81.40.14.213	Forniti ISP

APPENDICE D: Firewall – Packet Filter

Il WebShare 3G 244WN dispone di un sofisticato Packet Filter col quale riesce ad esaminare tutto il traffico che lo attraversa. In questo modo è possibile, conoscendo le caratteristiche dei pacchetti IP associati ai più comuni servizi, effettuare i filtraggi in maniera corretta. In questa appendice verranno evidenziate le varie modifiche subite da un pacchetto durante il percorso.

Verranno utilizzate le seguenti convenzioni:

- **BLU** per indicare una INVERSIONE
- **ROSSO** per indicare un CAMBIAMENTO

Condizioni di partenza:

- NAT attivo
- PCX della LAN con IP 192.168.1.X
- Router con LAN IP 192.168.1.254

Il caso da esaminare prevede una LAN in cui il PC con IP 192.168.1.X vuole visualizzare un sito WEB.

Vi sono 2 fasi:Risoluzione dell'URL (tale valore potrebbe essere recuperato in qualche cache o fornito da appositi programmi, ma per completezza verrà affrontato il caso più comune) e costruzione della connessione TCP col sito WEB.

Il primo pacchetto è inviato dal PC (con IP 192.168.1.X) verso il server DNS per chiedere la risoluzione dell'URL cercato.

	Direzione Pacchetto	PC-Router[Uscente]	
IP	IP Provenienza	192.168.1.X	
	IP Destinazione	IP del Server DNS	
	Pacchetto contenuto	Tipo UDP	UDP
	Porta Provenienza	C	
	Porta Destinazione	53	

Questo pacchetto uscente arriva al WebShare 141W che (essendo abilitato il NAT) ne cambia l'indirizzo di provenienza mettendo il suo IP Pubblico e lo inoltra al server DNS.

	Direzione Pacchetto	Router-Internet[Uscente]	
IP	IP Provenienza	**IP lato WAN del Router**	
	IP Destinazione	IP del Server DNS	
	Pacchetto contenuto	Tipo UDP	UDP
	Porta Provenienza	C	
	Porta Destinazione	53	

Arrivato al server DNS il pacchetto torna indietro, reindirizzato al WebShare 141W (che ne aveva cambiato prima l'IP di provenienza). Sono invertiti sia a livello IP i campi IP prov con IP dest e sia le porte nel livello UDP.

	Direzione Pacchetto	Internet-Router[Entrante]	
IP	IP Provenienza	**IP del Server DNS**	
	IP Destinazione	**IP lato WAN del Router**	
	Pacchetto contenuto	Tipo UDP	UDP
	Porta Provenienza	**53**	
	Porta Destinazione	**C**	

Arrivato al WebShare 3G 244WN, il pacchetto viene riprocessato ed inviato al PC di provenienza.

	Direzione Pacchetto	Internet-Router[Entrante]	
IP	IP Provenienza	IP del Server DNS	
	IP Destinazione	**192.168.1.X**	
	Pacchetto contenuto	Tipo UDP	UDP
	Porta Provenienza	53	
	Porta Destinazione	C	

A questo punto, dal pacchetto UDP arrivato, il PC (con IP 192.168.1.X) ha risolto l'URL e conosce l'indirizzo IP associato. Inizia dunque la fase della costruzione della connessione TCP (il protocollo TCP infatti richiede la costruzione della connessione, al contrario di quello UDP).

	Direzione Pacchetto	PC-Router[Uscente]	
IP	IP Provenienza	192.168.1.X	
	IP Destinazione	IP URL	
	Pacchetto contenuto	Tipo TCP	TCP
	Porta Provenienza	K	
	Porta Destinazione	80	

Questo pacchetto uscente arriva al Router che (essendo abilitato il NAT) ne cambia l'indirizzo di provenienza mettendovi il suo Pubblico e lo inoltra al server WEB.

	Direzione Pacchetto	Router-Internet[Uscente]	

IP	IP Provenienza	**IP lato WAN del Router**	
	IP Destinazione	IP URL	
	Pacchetto contenuto	Tipo TCP	TCP
	Porta Provenienza	K	
	Porta Destinazione	80	

Arrivato al server WEB il pacchetto torna indietro, reindirizzato all' WebShare ADSL2+ Router (che ne aveva cambiato prima l'IP di provenienza). Vengono invertiti sia a livello IP i campi IP prov con IP dest e sia le porte nel livello TCP.

	Direzione Pacchetto	Internet- Router [Entrante]	
IP	IP Provenienza	**IP URL**	
	IP Destinazione	**IP lato WAN del Router**	
	Pacchetto contenuto	Tipo TCP	TCP
	Porta Provenienza	**80**	
	Porta Destinazione	**K**	

Arrivato all' WebShare ADSL2+ Router il pacchetto viene riprocessato ed inviato all'IP di provenienza.

	Direzione Pacchetto	Router-PC[Entrante]	
IP	IP Provenienza	IP URL	

	IP Destinazione	**192.168.1.X**	
	Pacchetto contenuto	Tipo TCP	TCP
	Porta Provenienza	80	
	Porta Destinazione	K	

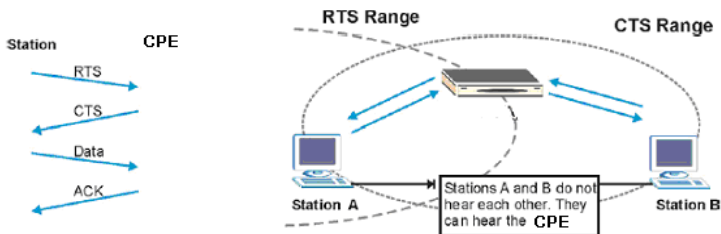
E’ stato evidenziato tanto il percorso dei pacchetti che le trasformazioni che questi subiscono. Nell’esempio di sopra si sono utilizzati dei parametri C e K. Sono dei numeri interi >1024. Nei protocolli per porta quali TCP/UDP infatti il mittente parla ad una porta di destinazione (su cui è in ascolto il server) ed indica una porta (la porta di provenienza appunto) dove aspetta la risposta. Il pacchetto una volta ricevuto dal server viene reinviato al mittente sulla porta su cui questo aspetta la risposta (viene effettuata un’inversione a livello di porte).

APPENDICE E: Introduzione ad una rete wireless

Introduzione alla rete Wireless
Questa sezione presenta la Wireless Lan e alcune configurazioni di base. Una Wireless Lan può essere creata semplicemente con due computer dotati di schede di rete Wireless che comunicano in una rete di peer-to-peer oppure in maniera più complessa utilizzando più computers con schede di rete senza fili che comunicano attraverso punti di accesso che fanno da ponte tra la rete Wireless e la rete cablata.

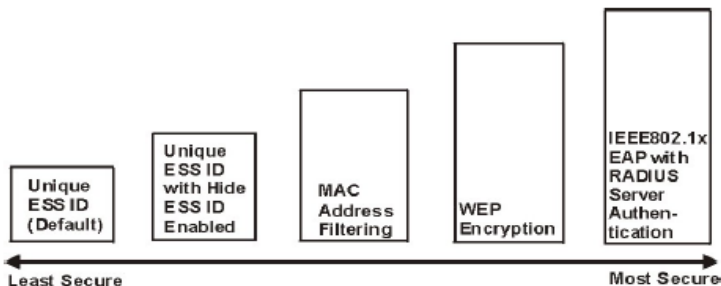
Canali
Il range di frequenze radio usate dalle apparecchiature Wireless IEEE 802.11b è suddiviso in "canali". Il numero di canali disponibili dipende dall' area geografica di appartenenza. E' possibile selezionare canali differenti in modo da eliminare eventuali interferenze con gli Access Point vicini. L'interferenza si verifica quando due o più canali si sovrappongono degradando le prestazioni, questa sovrapposizione è chiamata "Overlap".
E' consigliabile mantenere una distanza di 5 canali tra due utilizzati (es. AP1-canale 1, AP2-canale 6).

ESS ID
L' Extended Service Set (ESS) consiste in un gruppo di Access Point o Gateway Wireless connessi ad un LAN cablata sulla stessa subnet. Un ESS ID identifica univocamente ogni gruppo. Ciascun Access Point o Gateway Wireless e le stazioni Wireless a loro associate devono avere lo stesso ESSID.

RTS/CTS
Quando due stazioni Wireless sono all'interno del range dello stesso Access Point ma non si vedono direttamente si ha un "nodo nascosto". La figura che segue illustra questa situazione.

La stazione A invia dei dati al Router ADSL ma nel mentre non sa se la stazione B sta già utilizzando il canale. Se le due stazioni trasmettessero richieste di inizio trasmissione allo stesso tempo si avrebbero delle collisioni quando le informazioni giungono all'Access Point.
Il protocollo RTS/CTS (Request To Send/Clear to Send) è stato disegnato per prevenire le collisioni quando si verificano situazioni di "nodi nascosti". Un RTS/CTS definisce la dimensione massima del frame di dati che è possibile trasmettere prima che la prossima richiesta RTS/CTS sia inoltrata. Quando un frame di dati supera il valore di RTS/CTS impostato (tra 0 e 2432 bytes), la stazione che vuole trasmettere deve inviare un messaggio RTS all' Access Point per ottenere il permesso ad iniziare. L'Access Point invia quindi a tutte le altre stazioni della rete Wireless un messaggio CTS vietando loro la trasmissione di dati.

Fragmentation Threshold (Soglia di frammentazione)
Il Fragmentation Threshold è la dimensione massima di frammentazione dei dati (tra 256 e 2432 bytes) che può essere trasmessa in una rete Wireless prima che il Router ADSL effettui un ulteriore divisione in frames più piccoli.
Un alto valore di Fragmentation Threshold è indicato per reti esenti da interferenze, mentre per reti soggette ad interferenze e con un traffico molto elevato è preferibile optare per un valore più basso.
Se viene impostato un valore più basso dell'RTS/CTS i dati verranno frammentati prima della fase di handshake la quale non verrà effettuata.

Livello di Sicurezza

Le funzionalità di Wireless Security sono necessarie per proteggere le comunicazione tra stazioni Wireless , Access Point e la rete cablata.
La figura sotto indica i possibili livelli di sicurezza Wireless firniti dal Router ADSL. Il livello di sicurezza più alto conta sul protocollo EAP (Extensible Authentication Protocol) per l'autenticazione ed utilizza WEP con scambio di chiavi dinamico. Questo sistema richiede l'interazione con un server RADIUS (Remote Authentication Dial-In User Service) che offre servizi di autenticazione per stazioni Wireless.

Se none viene utilizzato alcuna funzionalità di Wireless Security il Router ADSL sara accessibile da qualsiasi stazione Wireless presente nel suo campo di azione. E' possibile configurare questo servizio tramite l'interfaccia di configurazione Web del prodotto.

Cifratura dati con WEP

La cifratura WEP provvede al crittaggio dei dati trasmessi sulla rete in modo da ottenere una comunicazione privata. Il crittaggio viene effettuato sia su comunicazioni unicast che multicast.
Tutte le stazioni Wireless che utilizzano questa cifratura devono utilizzare la stessa chiave per la cifratura e la decodifica dei dati. Il Wireless Router ADSL2+ è in grado di utilizzare chiavi di criptaggio da 64 e 128 bit.

APPENDICE F: Copertura

Considerazioni Generali

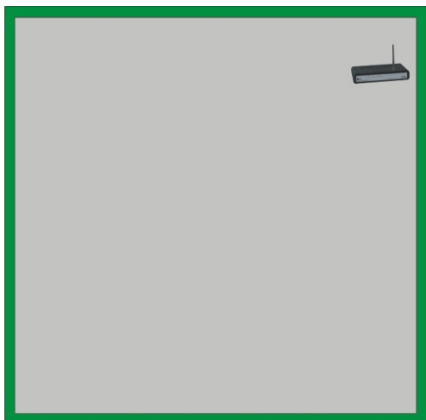
In condizioni ideali la copertura offerta dal dispositivo può arrivare anche a coprire diverse decine di metri. E' però opportuno considerare che pareti divisorie attenuano fortemente il segnale. Oggetti metallici riflettono le onde elettromagnetiche e possono generare (al pari di particolari ambienti indoor) fastidiosi cammini multipli. Non va trascurato inoltre il fenomeno dell'interferenza con altri apparati operanti sulle frequenze vicine.

Rispettare i seguenti punti per massimizzare la copertura offerta dal dispositivo.

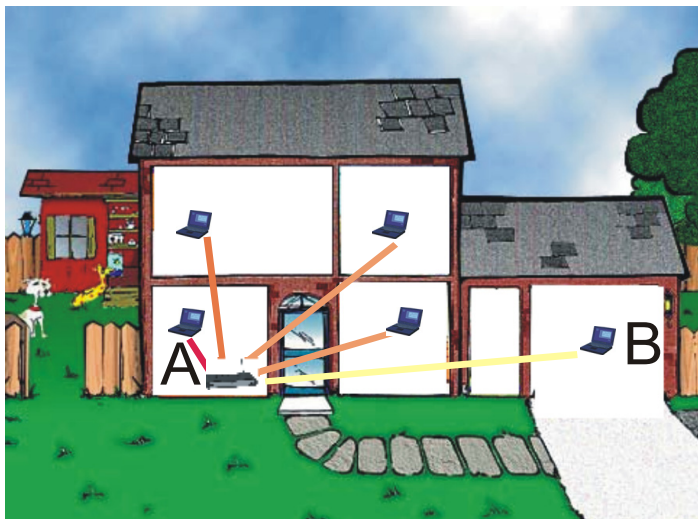
- Ogni muro attenua il segnale, posizionare il dispositivo in un luogo appropriato al fine di minimizzare il numero di muri attraversati dal segnale.

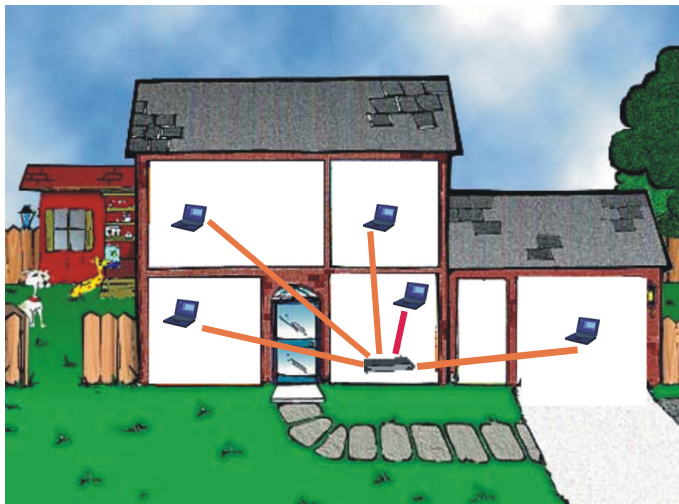
- Porte o ampie superfici metalliche non sono attraversate dalla propagazione elettromagnetica. E' bene prendere in considerazione questo fatto.

- Allontanare l'AP Wireless da ogni altro dispositivo che produca emissioni RF.

- Nel posizionamento dei vari client considerare una linea che idealmente unisce il Wireless AP col client in questione. Se tale linea intersecherà dei muri (caso assai frequente), cercare di minimizzare la superficie attraversata (per evitare di avere un'attenuazione importante). Si veda la figura sottostante:

Il Client in posizione B avrà un'enorme attenuazione e peggiori prestazioni che non il client in posizione A, benché la distanza effettiva dall'AP sia quasi identica nei 2 casi. E' sufficiente collocare il Wireless AP al centro del locale per migliorare decisamente le prestazione del client B.

Dove installare un AP

Immaginiamo di avere un'installazione come quella in figura.

Sicuramente Client in posizione B avrà un'enorme attenuazione e peggiori prestazioni che non il client in posizione A.

E’ sufficiente collocare il Wireless Router/AP al centro della rete per migliorare decisamente le prestazione di entrambi i client B.

Si è operato sulla diminuzione 2 fattori:

- Distanza media
- Sezioni di muro attraversate

E’ decisamente meglio avere una rete i cui client abbiano un link mediamente buono che non una rete con taluni client con link eccellente ed altri con link molto scarso.

La stazione lontana, che generalmente trasmette con un data rate più basso, tende a consumare un «airtime» elevato.

L’AP ha meno tempo da dedicare a client più vicini e più veloci.

Prestazioni complessivi peggiori.

APPENDICE G: Lista di compatibilità Modem 3G

Di seguito sono riportati i modem USB 3G testati e ritenuti pienamente compatibili con il WebShare 3G 244WN al momento della stesura del documento.

Brand	Model
Sierra	Aircard 880U
Sierra	Aircard 875U
Sierra	Aircard 885U
Huawei	E180
Huawei	E170
Huawei	E160G
Huawei	E169G
Huawei	E169
Huawei	E220
Huawei	E270
Huawei	E172
Huawei	E272
ZTE	MF626 NEW
ZTE	MF638
ZTE	MF628
ZTE	MF622

NOVATEL	MC950D
NOVATEL	MC930D NEW
NOVATEL	MC990D NEW
BandRich	Bandluxe C100
Alcatel	OT-X020
C-Motech	D50
Telstra	USB3-8521
Option	GlobeSurfer iCON 7.2 NEW
Option	iCON 225 NEW
Option	GlobeSurfer iCON HSUPA NEW
Option	GlobeTrotter HSUPA NEW

Una versiona costantemente aggiornata della lista di compatibilità è disponibile sul sito www.atlantis-land.com nella relativa sezione di prodotto.

APPENDICE H: Supporto

Per qualunque altro problema o dubbio sul funzionamento del prodotto, è possibile contattare il servizio di assistenza tecnica Atlantis Land tramite l'apertura di un ticket on-line sul portale http://www.atlantis-land.com/ita/supporto.php.

Nel caso non fosse possibile l'accesso al portale di supporto, è altresì possibile richiedere assistenza telefonica al numero 02/00632345.

Per esporre eventuali richieste di supporto prevendita o richieste di contatto , vi invitiamo ad utilizzare gli indirizzi mail info@atlantis-land.com oppure prevendite@atlantis-land.com.

Atlantis Land
Via Pelizza da Volpedo, 59
20092 Cinisello Balsamo (MI) - Italy
Tel: +39. 02.00.632.300
Fax: +39. 02.66.016.666
Website: http://www.atlantis-land.com
Email: info@atlantis-land.com